



Version: 18/August/2007

User Manual

Wireless

Decision Computer International Co., Ltd

Copyright © 2007 Decision Computer International Co., Ltd



IMPORTANT NOTICE

This guide is delivered subject to the following conditions and restrictions:

Copyright Decision Computer Ltd. 2007. All rights reserved.

The copyright and all other intellectual property rights and trade secrets included in this guide are owned by Decision Ltd. The guide is provided to Decision customers for the sole purpose of obtaining information with respect to the installation and use of the E-Detective System, and may not be used for any other purpose.

The information contained in this guide is proprietary to Decision and must be kept in strict confidence.

It is strictly forbidden to copy, duplicate, reproduce or disclose this guide or any part thereof without the prior written consent of Decision.

Table of Contents

Version: 18/August/2007.....	1
Introduction to Wireless E-Detective System.....	5
System Installation.....	8
System Setup.....	10
Remotely login.....	11
Wireless E-Detective System Functions.....	11
A. Local and Remote Login.....	11
B. Email Recording.....	14
1. POP3 [inbound]	14
2. SMTP [outbound].....	16
3. IMAP [inbound].....	17
4. WebMail.....	18
5. WebMail (Send).....	19
C. Chats.....	20
1. MSN.....	20
2. ICQ.....	21
3. YAHOO.....	22
4. QQ.....	23
5. VOIP	24
D. Website Log.....	26
1. HTTP - URL log.....	26
2. HTTP (Dynamic)-webpage content log.....	27
E. Telnet	28
F. FTP	29
G. P2P.....	30
H. Online Game.....	31
I. Search.....	32
1. Example (by IP):.....	33
1. Example (by IP & MSN).....	34
2. Special Search Type [only apply to MSN / ICQ / YAHOO].....	35
J. ALARM.....	39
K. Export.....	42
L. Wireless	44
Wireless Network Management.....	44
2. Import.....	53
3. WEP key.....	54

4. History.....	55
5. Work Log.....	56
6. IDS (Intrusion Information).....	57
M. Backup Data.....	58
1. Backup Raw Data (ISO).....	58
2. Backup (Database).....	59
N. SYSTEM.....	60
1. Network Setup.....	60
2. HDD Usage.....	64
3. Server.....	65
4. Set up System Time.....	67
O. Network Users.....	68
1. On-line IP information.....	68
2. List of Logged-in Users.....	72
3. Nbns.....	73
P. Authority Setup.....	74
1. Group Setup.....	74
2. Create user.....	76
Q. Delete Data.....	77
1. Delete (Mode).....	77
2. Delete (All)	78
R. EDIT PASSWORD	79
S. POWER ON/OFF.....	80
T. QQ INFO. SETUP (How to see the encrypted conversation).....	81
Step 1 – Download the QQ cracker:	81
Step 2 – Install QQ cracker into computer.....	81
Step 3 – Decrypt the conversation.....	85
U. GPS.....	89
B.....	89
V. Data Mining.....	90
Appendix A: Q & A.....	92

Introduction to Wireless E-Detective System

Internet application becomes more and more popular by the emergence of broadband Internet. Popular but unregulated Internet access has caused a challenge to the management. Wireless E-Detective system can sniff and decode Internet activities through Wireless LAN (WLAN) such as emailing (POP3, SMTP, IMAP, Web Mails), chatting (Yahoo, MSN, ICQ, AOL, QQ), HTTP/URL Web Browsing and Files Transfer (FTP) upload and download, P2P upload and download, Telnet, Online Games, VOIP and Webcam (MSN and Yahoo) etc. E-Detective system can improve corporate efficiency, prevent network resources from being misuse, guide network administrator to block the loophole of confidential information leakage, monitor cyber-slacker and avoid accidental deleting and damage of email (recover from backup).

Network Sniffing is one of the important the way to preserve evidence. It will duplicate every Internet activity and data transferred, and it also needs a powerful system like E-Detective to perform online Internet sniffing, real-time recording, categorizing, correct misbehavior, data mining, statistics analysis, etc.

Wireless E-Detective system adopts optimized Linux as the kernel and plus powerful Java Applet to provide a complete graphical interface for user. User can configure and use on the fly (Plug & Play). Wireless E-Detective's speedy packet sniffing technology can sniff on specific target or scope (selecting wireless devices with similar channel) without interfering original network environment.

Since wireless access to Internet has been very popular in everywhere, Wireless E-Detective system can be used by police, military, information investigation and forensic departments to track down illegal internet activities such as illegal betting, transactions, access and others.

Product Benefits:

Emails [POP3, SMTP, IMAP, Web Mail]	Automatically sniff and back up incoming & outgoing e-mail (including Hotmail and other Web Mail), anonymous user and attachment for tracking leakages down to insure security.
Internet Chatting [MSN, ICQ, YAHOO, AOL, QQ]	Faithfully sniff and record chatting contents, user's name, account and IP.
File upload & download (FTP)	Back up uploaded and downloaded files for management and tracking.
Website (HTTP)	Monitor and capture all websites browsed including updates to Windows, Anti virus etc.
P2P upload & download	Monitor and capture all P2P Communications (upload and download) sessions like port used, peer's IP address, peer's port address etc.
Online games	Monitor and capture all Online Game sessions such as Kartrider, Ragnarok Online, World of Warcraft etc.
Decryption of WEP key	Capable to decrypting WEP key of length 64, 128 bits with enough packets captured.
Warning message and remote monitoring	Set up warning policy: collect the data that meets warning policy and send warning mail to designated account, also can remotely monitor via browser at the same time.
Powerful Search and Data Mining	Capable of Search by different applications and data mining by keywords.
Easy installation	Easy operation; one main unit can provide full-scale services.

System Setup and Implementation

Wireless E-Detective system uses sniffer mode to sniff wireless network packets ranging from 0 – 100 meters depending on the environment setup. For indoor environment with walls, furniture blockage, the coverage range could be reduced. For outdoor with very less blockage and line of sight, the coverage range is more. Higher gain antenna can be used to extend the coverage range of sniffing wireless packets.



Figure: Wireless E-Detective System sniffs wireless packets from WLAN network

System Installation

Please follow the following steps for system installation:

1. Switch in the power supply and the Wireless E-Detective system.
2. Insert the Installation CD into the CD ROM.
3. Set from BIOS of the system to boot 1st from CD-ROM.
4. Reboot the system.
5. The installation CD will automatically start the installation process.
6. If you see the following message, the installation process will stop:
Accept or Don't ? Please answer (Yes/No) : yes
Now starting to install E-Detective System.....
This version is Unlimited.

***** HardDisk Configuration *****

Do you want to continue ? yes

1 : hdc : ASUS CRW-5232AS, ATAPI CD/DVD-ROM drive

2 : hdc : ATAPI 52X CD-ROM CD-R/RW drive, 2048kB Cache, UDMA(33)

Please answer (Yes/No) : yes

Please input YES to continue or NO to stop the Installation process.

7. After the installation complete, you will see the following setup:

Local login :

Username : root

Passwd : 111111

Remote login :

Username : root

Passwd : 000000

Default IP : 192.168.1.60

Copyright © 2007 Decision Computer International Co., Ltd

Default GW : 192.168.1.1

Please press Ctrl-Alt-Delete to restart the system.

If you need reset E-Detective server's IP,
please excute " SetIP " after local login.

hd = /dev/hda, hd1 = (null), cdrom = hdc, status = 2

WARNING : could not determine runlevel - doing soft reboot

(it's better to use shutdown instead of reboot from the command line)

shutdown : No such file or directory

/bin/eject : unable to find or open device for : "cdrom"

BusyBox v.0.60.3 (2002.06.20-18 : 01+0000) Built-in shell (ash)

Enter " help " for a list of built-in commands.

sh : can't access tty ; job control turned off.

#

Note: Please reboot the system and extract out the installation CD. If not, the system will always boot from the CD-ROM and repeat the installation.

System Setup

E-Detective System default IP is 192.168.1.60, default Gateway is 192.168.1.1. If you would like to change the IP, there are two ways to change.

Locally Login

Note: Change/Set IP locally is done by connecting a Monitor and Keyboard to the E-Detective system.

User can login locally using username: root and password: 111111 to configure SetIP configuration as follow:

```
debian:~# SetIP
IP(192.168.1.59): 192.168.1.59
Netmask(255.255.255.0):
Broadcast(192.168.1.255):
Gateway(192.168.1.1):
You have entered the following network information:
IP      : 192.168.1.59
Network : 255.255.255.0
Broadcast: 192.168.1.255
Gateway : 192.168.1.1
Is the information correct? (Yes/No): Yes
```

On screen will show the following message (IP, Network, Broadcast, Gateway), identify where the information is correct, if so enter "Yes" to complete the IP setup. The following message will then be shown:

```
MAN_NIC: eth0
SSH PORT: 22
Reset OK!
Broadcast message from root (pts/0) (Fri Jun  2 17:01:46 2006):

The system is going down for reboot NOW!

Broadcast message from root (pts/0) (Fri Jun  2 17:01:46 2006):

The system is going down for reboot NOW!
debian:~#
```

Remotely login

User can remotely login using username: root and password: 000000. Before login to E-Detective system, make sure the user PC is within the same subnet as E-Detective system. After login, please select [Manage], [System], [Network Setting], and [Setup] to configure the IP. After completed the setting of IP, please click [Submit] and [Finished]. The system will restart to complete the IP setup.

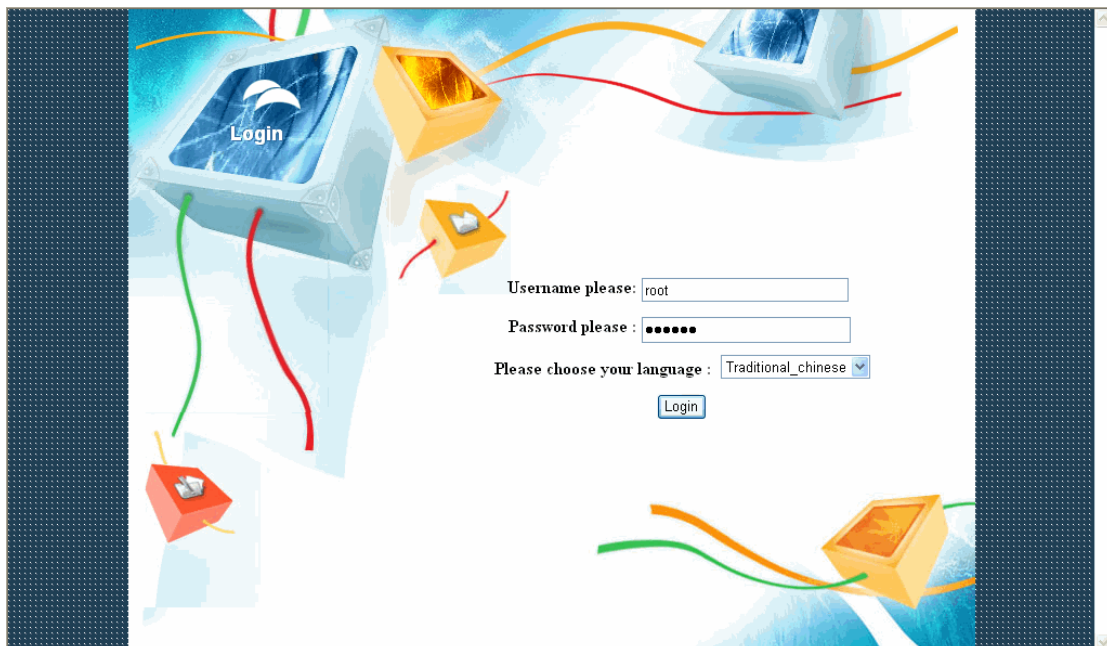
Wireless E-Detective System Functions

A. Local and Remote Login

- For local login, the default URL is: **https://192.168.1.60**
- For both local and remote login, please input default user's name: **root**
- Default password: **000000**
- Language: Selecting preferred language.
- Press the button [**Login**] to log in system.

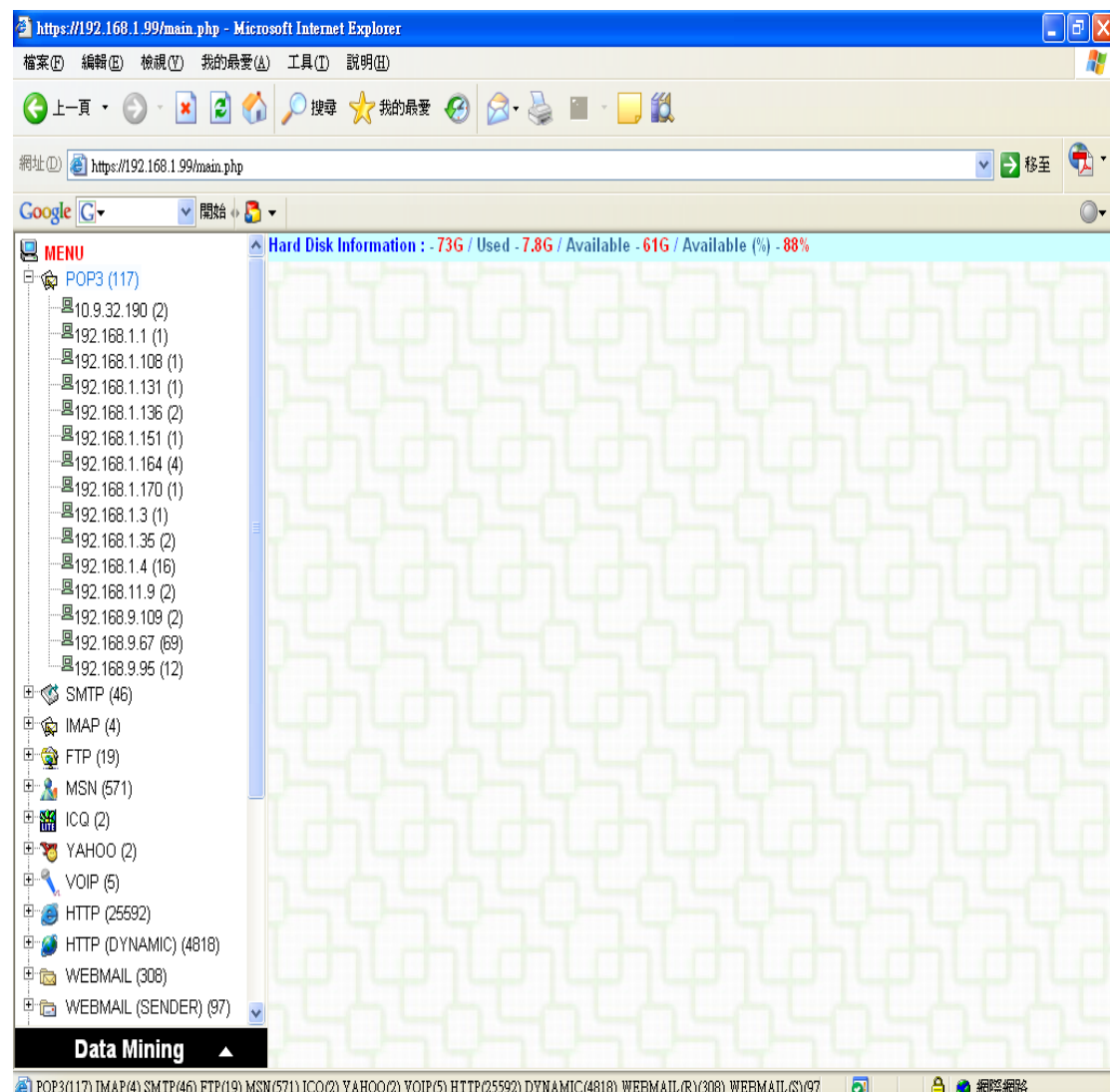


Press Yes button



The navigation bar listed on the left panel, it shows all functionalities and targets' IP. Users click the targets' IP to see the records captured.

There is statistical number after category (POP3, SMTP, FTP, HTTP, etc.). That number means the total records captured and belonged to the particular category or target's IP. Ex: POP3 (48), POP (117)



B. Email Recording

Emails recording supports :

1. POP3 [inbound]
2. IMAP [inbound]
3. SMTP [outbound]
4. Webmail [inbound]
5. Webmail (send) [outbound]

1. POP3 [inbound]

POP3 [inbound] records detailed information of each received e-mail, including full text analysis, receiving date, time, sender, receiver's IP, receiver, carbon copy, topic, account, password and attachment. All POP3 emails running on applications such as Outlook Express, Microsoft Office Outlook and etc. will be captured in the Wireless E-Detective System.

NO.	@	DATE / TIME	FROM	TO	CC	SUBJECT	ACCOUNT	PASSWOR
1.		2007-02-02 15:44:47	frankie@deci...	service@deci...	vincent@...	↓ RE: Request for update version of Wi...	service@...	yrhhi8
2.		2007-02-02 15:44:47	tony@tsuensh...	service@deci...	printk@g...	↓ RE: RE: FW: Feedback From Decision	service@...	yrhhi8
3.		2007-02-02 15:44:47	casper@decis...	service@deci...	NONE	↓ FW: Edetective	service@...	yrhhi8
4.		2007-02-02 15:44:47	decision@dec...	service@deci...	NONE	↓ Fw: Question	service@...	yrhhi8
5.		2007-02-02 15:44:47	tony@tsuensh...	service@deci...	NONE	↓ FW: Feedback From Decision	service@...	yrhhi8
6.		2007-02-02 15:44:47	printk@gmail...	service@deci...	NONE	↓ Re: Feedback From Decision	service@...	yrhhi8
7.		2007-02-02 15:44:47	jim@pengo.co...	service@deci...	michael@...	↓ RE: RE: ED system	service@...	yrhhi8

Features in this user interface (UI):

- [1] : Attachment: There will be a symbol appeared if there is more than one attachments included.
- [2] : Download: A link to download the record.
- [3] : Subject: Click on e-mail's subject to see the content.

View Email Content:

The following diagram is popped up if user clicks the subject name.

Subject	Make the payment
From	service@decision.com.hk
To	whoopshank@dec
CC	
BCC	
Date	2007-02-02 14:59:10.0
Source	POP3 sbiPNz eml tat
Attachment	DVC00491.JPG
IP	192.168.9.95
DATETIME	2007-02-02 15:40:07.0

click this link to see the source
code of this webpage

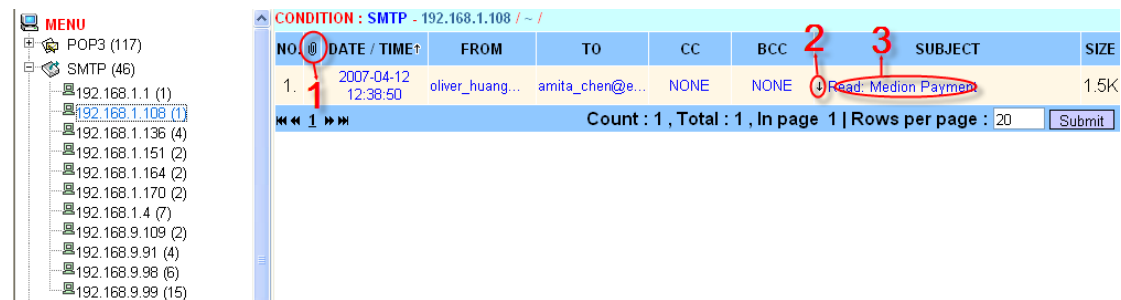
click this link to see
the attached file

Hi Tony~

The Decision company does not have the information of Tsuen Shing and your seller (SIB). That is why it took time to reply you and resulted in this unwanted delay.

2. SMTP [outbound]

SMTP [outbound] records detailed information of each received e-mail, including full text analysis, receiving date, time, sender, receiver's IP, receiver, carbon copy, topic and attachment. All SMTP emails running on applications such as Outlook Express, Microsoft Office Outlook and etc. will be captured in the Wireless E-Detective System.

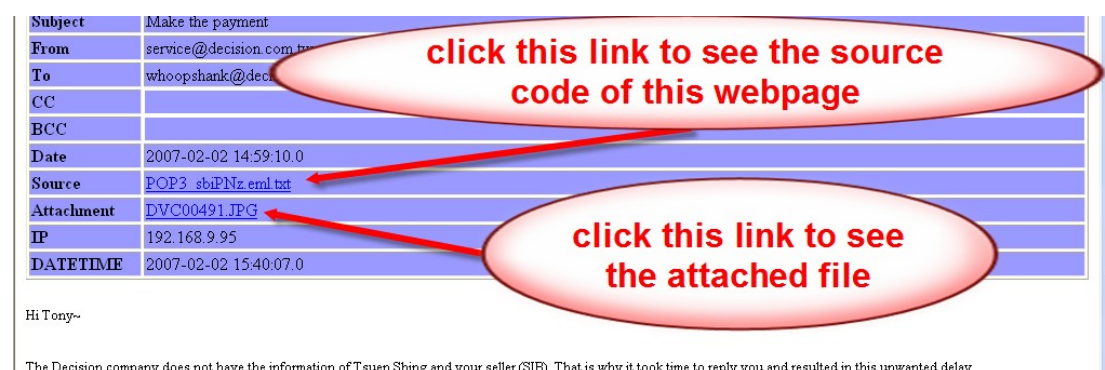


Features in this user interface (UI):

- [1] : Attachment: There will be a symbol appeared if there is more than one attachments included.
- [2] : Download: A link to download the record.
- [3] : Subject: Click on e-mail's subject to see the content.

View Email Content:

The following diagram is popped up if user clicks the subject name.



3. IMAP [inbound]

IMAP [inbound] records emails when targets use IMAP email server. The details of email recorded include date, time, sender address, receiver address, CC, BCC, user account and password as shown in diagram below.

NO.	DATE / TIME	FROM	TO	CC	SUBJECT	ACCOUNT	PASSWORD
1.	2006-10-20 13:27:16	whoopshank@d...	happycall.tw...	NONE	News for you	happycal...	password
2.	2006-10-20 13:27:16	service@deci...	whoopshank@d... happycal...		You must read this newz	whoopsha...	whoops
3.	2006-10-20 13:27:16	hsieh@yahoo...	ivan@hotmail...	NONE	Have you read this news ?	ivan	ivan2233
4.	2006-10-20 13:27:16	leo@network...	leo@yahoo.co...	NONE	This information you must know ...	leo	leoyou

Count : 4 . Total : 1 . In page 1 | Rows per page : 20 | Submit

Features in this user interface (UI):

- [1] : Attachment: There will be a symbol appeared if there is more than one attachments included.
- [2] : Download: A link to download the record.
- [3] : Subject: Click on e-mail's subject to see the content.

View Email Content:

The following diagram is popped up if user clicks the subject name.

Subject Make the payment
From service@decision.com.tw
To whoopshank@dec...
CC
BCC
Date 2007-02-02 14:59:10.0
Source [POP3 sbIPNz.eml.txt](#)
Attachment [DVC00491.JPG](#)
IP 192.168.9.95
DATETIME 2007-02-02 15:40:07.0

Hi Tony~

The Decision company does not have the information of Tsuen Shing and your seller (SIB). That is why it took time to reply you and resulted in this unwanted delay.

4. WebMail

WebMail log includes the information of date, time, user's IP, webmail contents and the type of mail server

Within log, E-Detective System will record text of WebMail only and filter out non-text to reduce HDD usage and system loading.

CONDITION: WEBMAILR - 192.168.1.164 (-)

NO.	DATE / TIME	URL	WEBMAIL TYPE
1.	2007-04-04 17:17:44	by12264 bay122 hotmail.msn.com R O	hotmail
2.	2007-04-04 17:17:44	by12264 bay122 hotmail.msn.com R O	hotmail
3.	2007-04-04 17:17:44	by12264 bay122 hotmail.msn.com R O	hotmail

Count: 3, Total: 3, In page 1 | Rows per page: 20

click link [O] to view the webmail content

Features in this user interface (UI):

[1] :  Download: A link to download the record.

[2] :  Source code: A link to view the source code of webpage.

Note: Users do not care about the links of subject name and R

5. WebMail (Send)

WebMail (send) log includes the information of date, time, sender, receiver, carbon copy, confidential carbon copy, subject, email contents and type of mail server.



The screenshot displays a WebMail interface. On the left, a sidebar shows a list of folders: 'WEBMAIL (SENDER)' with sub-folders for IP addresses (192.168.1.78, 192.168.1.84, 192.168.9.109, 192.168.9.91), 'TELNET (12)', 'QQ (3)', and 'P2P (0)'. The main area shows a table of sent emails with columns: NO., DATE / TIME, FROM, TO, CC, BCC, SUBJECT, and WEBMAIL TYPE. Three rows of data are visible, each with a red arrow pointing to a specific feature: [1] points to a download icon in the 'NO.' column, [2] points to a source code icon in the 'BCC' column, and [3] points to an attachment icon in the 'SUBJECT' column. Below the table, a detailed view of an email is shown with fields for FROM, DATE / TIME, TO, SUBJECT, and ATTACHMENT. A red arrow points from the 'SUBJECT' field in the table to the 'SUBJECT' field in the detailed view, with the text 'click subject to view the email'.

NO.	DATE / TIME	FROM	TO	CC	BCC	SUBJECT	WEBMAIL TYPE
1.	2006-11-02 12:23:34	valenthsu9999...	ken@decision...	NONE	NONE	Yahoo - 測試信 3	yahoo
2.	2006-11-02 12:23:14	valenthsu9999...	ken@decision...	NONE	NONE	Yahoo - 測試信 2	yahoo
3.	2006-11-02 12:22:53	valenthsu9999...	ken@decision...	NONE	NONE	Yahoo - 測試信 1	yahoo

FROM :0952036619@ms66.url.com.tw
DATE / TIME :2006-11-03 10:21:34
TO :ken@decision.com.tw
SUBJECT :URL - 測試信 6
ATTACHMENT :
URL - 測試信 6

click subject to view the email

Features in this user interface (UI):

- [1] : Download: A link to download the record.
- [2] :  Source code: A link to view the source code of webpage.
- [3] :  Attachment: There will be a symbol appeared if there is more than one attachments included.

C. Chats

Chat messages are captured while targets use one of the Instant Messengers such as Yahoo, MSN, ICQ, AOL and QQ.

1. MSN

MSN log includes the information of date, time, chatter's accounts, and number of messages and transferred file.

click link [CONVERSATION] to view the messages.

NO.	DATE / TIME	SCREEN NAME	PARTICIPANTS	CONVERSATION	COUNTS
1.	2007-04-04 17:17:19	senica@decision.com.tw	raymondjlin@hotmail.com	CONVERSATION	3

Count: 1, Total: 1, In page 1 | Rows per page: 20 | Submit

DATE / TIME	SCREEN NAME	FILE NAME	SIZE	MESSAGE
2007-04-04 17:17:21	senica@decision.com.tw		91	
2007-04-04 17:17:22	raymondjlin@hotmail.com			Hello
2007-04-04 17:18:05	raymondjlin@hotmail.com			你好

Count: 3, Total: 1, In page 1 | Rows per page: 20 | Submit

Features in this user interface (UI):

- [1] : COUNTS: The total number of messages.
- [2] : FILE NAME: An icon will be appeared if there is a transmitted file, user clicks on that icon to view/download that file.

2. ICQ

ICQ log includes the information of date, time, chatters' IDs, and number of messages and transferred file.

The screenshot displays the ICQ log interface. At the top, a menu on the left lists various services: POP3 (117), SMTP (46), IMAP (4), FTP (19), MSN (571), and ICQ (2). The main window shows a list of conversations with columns: NO., DATE / TIME, SCREEN NAME, PARTICIPANTS, CONVERSATION, and COUNTS. The first conversation is selected, showing a count of 13. A red arrow points from the 'CONVERSATION' column to a detailed view of the conversation below. This detailed view has columns: DATE / TIME, SCREEN NAME, FILE NAME, SIZE, and MESSAGE. A red arrow points from the 'FILE NAME' column to a specific row. The detailed view shows a list of messages and files transferred.

click the link [CONVERSATION] to view the dialogue

1

2

NO.	DATE / TIME	SCREEN NAME	PARTICIPANTS	CONVERSATION	COUNTS
1.	2007-01-31 09:07:41	207706947	386490766	CONVERSATION	13

Count: 1, Total: 1, In page 1 | Rows per page: 20

DATE / TIME	SCREEN NAME	FILE NAME	SIZE	MESSAGE
2007-01-31 09:07:41	207706947			King Abdullah II of Jordan, right, with Palestinian Authority President Mahmoud Abbas, on Tuesday.
2007-01-31 09:07:49	207706947			Washington state snowed under, iced over.
2007-01-31 09:07:54	207706947			Bush: No pullout until 'mission is complete'
2007-01-31 09:07:58	207706947			Chomping sea lions terrorizing swimmers.
2007-01-31 09:08:02	207706947			Parents of fast-maturing 'tweens' seek balance.
2007-01-31 09:08:06	207706947			'Skate park on snow' lures youth to the slopes.
2007-01-31 09:08:09	207706947			Schools, teachers fight 'No Child Left Behind' in court.
2007-01-31 09:08:13	207706947			NATO allies grumble over Afghan mission.
2007-01-31 09:08:17	207706947			Pelosi looks past Hastings for intelligence committee post
2007-01-31 09:08:22	207706947			Study: 'Violent video game effects linger in brain.'
2007-01-31 09:09:55	207706947			881....
2007-01-31 09:10:03	386490766			886.....
2007-01-31 09:10:07	386490766			??????????????

Count: 13, Total: 1, In page 1 | Rows per page: 20

Features in this user interface (UI):

[1] : COUNTS: The total number of messages.

[2] : FILE NAME: An icon will be appeared if there is a transmitted file, user clicks on that icon to view/download that file.

3. YAHOO

YAHOO log includes the information of date, time, chatters' IDs and transmitted files.

The screenshot displays the YAHOO log interface. At the top, a menu on the left lists various protocols: POP3 (117), SMTP (46), IMAP (4), FTP (19), MSN (571), ICQ (2), and YAHOO (2). The main area shows a table of conversations. The first row is highlighted, showing a conversation with ID 1, dated 2007-01-31 09:07:41, screen name 207706947, and participants 386490766. The 'CONVERSATION' column is circled in red, and a red arrow points to it with the text 'click the link [CONVERSATION] to view the dialogue'. The 'COUNTS' column shows 13, which is also circled in red. Below this, a detailed view of the conversation is shown, with a 'FILE NAME' column circled in red and a red arrow pointing to it with the number '2'. The detailed view shows a list of messages with their dates, times, screen names, file names, sizes, and messages. The messages are news headlines. The bottom of the interface shows a summary: 'Count: 13, Total: 1, In page: 1 | Rows per page: 20'.

NO.	DATE / TIME	SCREEN NAME	PARTICIPANTS	CONVERSATION	COUNTS
1.	2007-01-31 09:07:41	207706947	386490766	CONVERSATION	13

Count: 1, Total: 1, In page: 1 | Rows per page: 20

DATE / TIME	SCREEN NAME	FILE NAME	SIZE	MESSAGE
2007-01-31 09:07:41	207706947			King Abdullah II of Jordan, right, with Palestinian Authority President Mahmoud Abbas, on Tuesday.
2007-01-31 09:07:49	207706947			Washington state snowed under, iced over.
2007-01-31 09:07:54	207706947			Bush: No pullout until 'mission is complete'
2007-01-31 09:07:58	207706947			Chomping sea lions terrorizing swimmers.
2007-01-31 09:08:02	207706947			Parents of fast-maturing 'tweens' seek balance.
2007-01-31 09:08:06	207706947			'Skate park on snow' lures youth to the slopes.
2007-01-31 09:08:09	207706947			Schools, teachers fight 'No Child Left Behind' in court.
2007-01-31 09:08:13	207706947			NATO allies grumble over Afghan mission.
2007-01-31 09:08:17	207706947			Pelosi looks past Hastings for intelligence committee post.
2007-01-31 09:08:22	207706947			Study: 'Violent video game effects linger in brain.
2007-01-31 09:09:55	207706947			881.....
2007-01-31 09:10:03	386490766			886.....
2007-01-31 09:10:07	386490766			??????????????

Count: 13, Total: 1, In page: 1 | Rows per page: 20

Features in this user interface (UI):

[1] : COUNTS: The total number of messages.

[2] : FILE NAME: An icon will be appeared if there is a transmitted file, user clicks on that icon to view/download that file.

4. QQ

QQ log includes the information of date, time, chatters' IDs and dialogue.

The screenshot displays a web-based QQ log interface. At the top, there's a status bar showing 'Hard Disk Information: -736 / Used -7.86 / Available -616 / Available (%) -88%'. Below this is a table listing conversations. The table has columns: NO., DATE / TIME, SCREEN NAME, PARTICIPANTS, CONVERSATION, and COUNTS. Two conversations are listed. The second conversation is highlighted, and a red circle is drawn around the word 'CONVERSATION' in its row. A red arrow points from this circle to a detailed view of the conversation below. The detailed view shows a table with columns: DATE / TIME, SCREEN NAME, TYPE, MESSAGE, START TIME, and END TIME. The first row of the detailed view shows a message from screen name 318624984 at 2006-11-06 10:52:18. The second row shows a message from screen name 572670102 at 2006-11-06 10:53:12. A red arrow also points from the 'COUNTS' column of the second conversation in the top table to the number '58' in the detailed view table. A red arrow points from the text 'click the link [CONVERSATION] to view the dialogue' to the 'CONVERSATION' link in the top table. A red arrow points from the number '1' to the 'COUNTS' column header in the top table.

NO.	DATE / TIME	SCREEN NAME	PARTICIPANTS	CONVERSATION	COUNTS
1.	2007-02-26 13:51:29	318624984	10000, ...	CONVERSATION	60
2.	2006-11-06 10:52:18	318624984	572670102	CONVERSATION	58

Count: 2, Total: 1, In page 1 | Rows per page: 20 Submit

click the link [CONVERSATION] to view the dialogue

DATE / TIME	SCREEN NAME	TYPE	MESSAGE	START TIME	END TIME
2006-11-06 10:52:18	318624984	MESSAGE	嘿嘿		
2006-11-06 10:52:18	318624984	MESSAGE	嘿嘿		
2006-11-06 10:52:22	318624984	MESSAGE	这个东西吧		
2006-11-06 10:52:22	318624984	MESSAGE	这个东西吧		
2006-11-06 10:53:12	572670102	MESSAGE	嘿嘿嘿嘿 还是希望 你会出现 送我出发		

Features in this user interface (UI):

[1] : COUNTS: The total number of messages.

5. VOIP

Before viewing the VOIP and webcam recorded, user has to set up the virtual environment on the following WEBCAM VOICE SETUP page.

Virtual environment requirements:

- An MSN account needs to be created for E-Detective system as E-Detective system need to connect online to MSN server to prompt the viewer message to listen to the VOIP session or view the webcam session.
- A viewer's MSN account (normally administrator's MSN account) for online viewing of the captured VOIP and Webcam sessions.

WEBCAM VOICE SETUP:

192.168.88.148 (1) Hard Disk Information : - 90G / Used - 264M / Available - 85G / Available (%) - 99%

WEBCAM VOICE SETUP

Ed Msn Account :	wedetective@hotmail.com
Ed Msn Password :	12345678
Viewer Msn Account :	wedetective1@hotmail.com

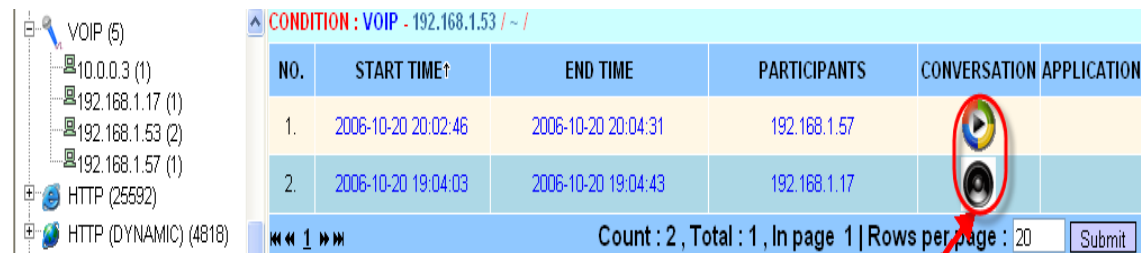
Submit



Features in this user interface (UI):

- ED MSN Account & Password:
Apply for a new msn email account and its password at Msn website for E-Detective system.
- Viewer Msn Account:
Setup the email account which the user uses to view the video.

VOIP:

VOIP (for MSN application) includes the information of start time, end time, participants' IPs, video and audio. (Setup the virtual environment first in order to view the video. Please refer to WEBCAM VOICE SETUP section for more detail).



NO.	START TIME	END TIME	PARTICIPANTS	CONVERSATION	APPLICATION
1.	2006-10-20 20:02:46	2006-10-20 20:04:31	192.168.1.57		
2.	2006-10-20 19:04:03	2006-10-20 19:04:43	192.168.1.17		

Count : 2 , Total : 1 , In page 1 | Rows per page : 20 Submit

click icons to view/hear video/audio.

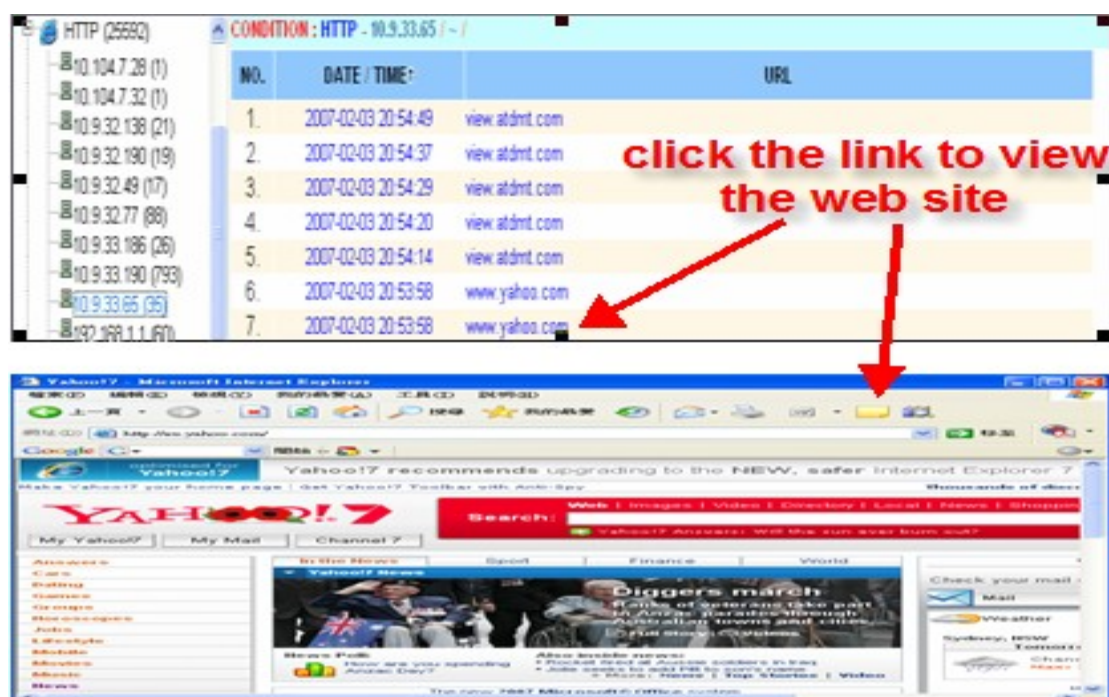
D. Website Log

E-Detective system captures the URLs and webpage's content that have been surfed.

1. HTTP - URL log

HTTP includes the information of date, time, user's IP and URL.

User clicks on the URL, the system will link to correspondent Web page [PC needs to be Internet-ready].



2. HTTP (Dynamic)-webpage content log

HTTP (Dynamic) includes the information of date, time, user's IP, URL and contents.



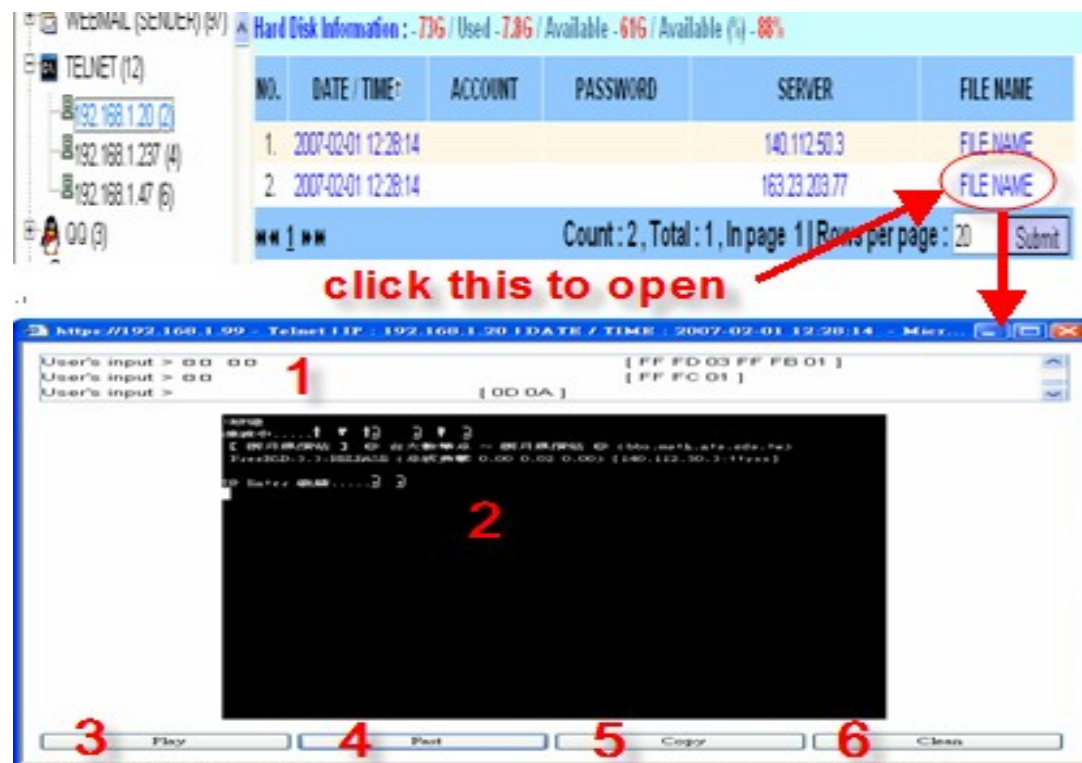
Features in this user interface (UI):

[1] : Source code: A link to view the source code of webpage.

Note: Users do not care about the links of subject name and R

E. Telnet

E-Detective System records the process from stem to stern while targets surf the internet via Telnet. Telnet includes the information of date, time, user account and password and server IP. The process from stem to stern saved into a file called "FILENAME". Users click the link 'FILENAME' to pop up a player to see the process.



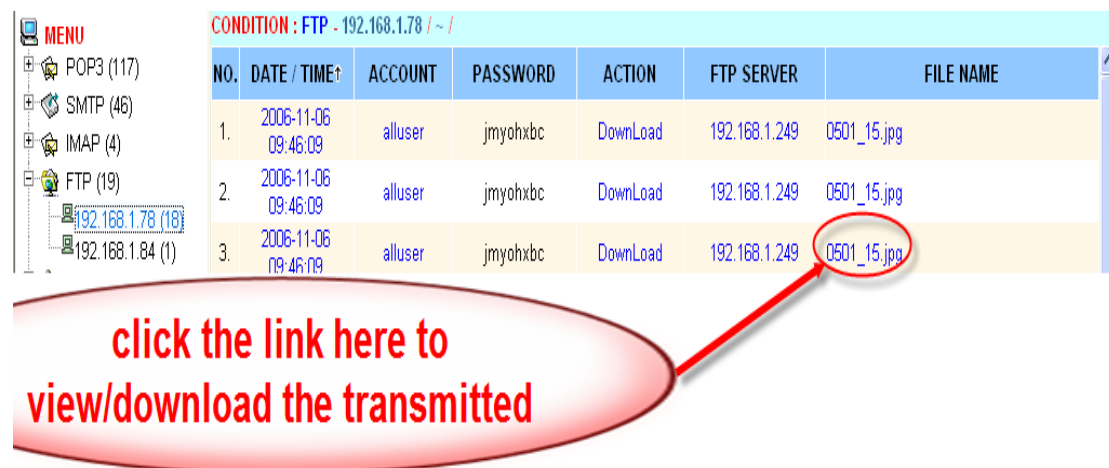
Features in this user interface (UI):

- [1] : A field to show the target's input.
- [2] : Black screen to show the content.
- [3] : Play button: To show the information once a character.
- [4] : Fast button: To show the information once a line.
- [5] : Copy button: User selects the user input first and then presses the copy button to get a copy.
- [6] : Clean button: To clear up the information on the black screen.

F. FTP

E-Detective system captures the transmitted files while targets use FTP to transfer the files.

FTP log includes information of date, time, user's IP, user's name, password and transmitted files shown as the following diagram.



CONDITION : FTP - 192.168.1.78 / ~ /

NO.	DATE / TIME	ACCOUNT	PASSWORD	ACTION	FTP SERVER	FILE NAME
1.	2006-11-06 09:46:09	alluser	jmyohxbc	DownLoad	192.168.1.249	0501_15.jpg
2.	2006-11-06 09:46:09	alluser	jmyohxbc	DownLoad	192.168.1.249	0501_15.jpg
3.	2006-11-06 09:46:09	alluser	jmyohxbc	DownLoad	192.168.1.249	0501_15.jpg

click the link here to view/download the transmitted

G. P2P

Peer to Peer (P2P), two computers are directly connected for transmitting the data without going through anyone else.

No.	DATE/TIME	PORT	P-IP	P-PORT	TOOL	FILENAME	ACTION	HASH
1.	2007-04-26 09:42:38	2680	75.62.239.184	14376	BitTorrent		DOWNLOAD	0207d788ed
2.	2007-04-26 09:42:33	2680	75.62.239.184	14376	BitTorrent		DOWNLOAD	0207d788ed
3.	2007-04-26 09:38:07	2680	75.62.239.184	14376	BitTorrent		DOWNLOAD	0207d788ed

Count : 3 , Total : 1 , In page 1 | Rows per page : 20 Submit

Features in this UI:

- [1] : IP: The target's IP at where you capture the data from.
- [2] : P-IP: The IP address where: the target transfers the data to.
- [3] : P-Port: Shows what port number used by second party.
- [4] : Tool: Shows what tool the targets use to transfer the data.
- [5] : File name: Show the transmitted file name.
- [6] : HASH: An identifiable value to identify which file is to be downloaded from specific second party.

H. Online Game

E-Detective system captures Online Game logs which include user's login date and time, user's MAC address, user's port number, Game Server IP address (P-IP), Game Server port number (P-PORT), and Game Name.

編號	日期/時間↑	MAC	PORT	P-IP	P-PORT	GAME NAME
1.	2007-07-03 09:20:22	00:13:ce:69:c7:31	2095	210.208.86.12	80	Kartrider
2.	2007-07-03 02:45:28	00:13:ce:69:c7:31	3279	210.208.86.12	80	Kartrider
共 : 2 筆, 共 : 1 頁, 目前第 1 頁 每頁幾筆 : <input type="text" value="20"/> <input type="button" value="送出"/>						

The Online Game logs that can be captured by E-Detective system are like World of Warcraft (WOW), Kartrider, Ragnarok Online etc.

I. Search

The system provides an advanced searching function. You may search by defined criteria.

SEARCH CONDITION		APPLY MODULE
DATE :	<input type="text"/> ~ <input type="text"/>	ALL
TIME :	<input type="text"/> : <input type="text"/> : <input type="text"/> ~ <input type="text"/> : <input type="text"/> : <input type="text"/>	
IP :	<input type="text"/>	
BSSID :	<input type="text"/>	
MAC :	<input type="text"/>	
EMAIL :	<input type="text"/> <input type="checkbox"/> FROM <input type="checkbox"/> TO <input type="checkbox"/> CC <input type="checkbox"/> BCC	
SUBJECT :	<input type="text"/>	
WEBMAIL TYPE :	<input type="text"/>	
FTP SERVER IP :	<input type="text"/>	
FTP ACCOUNT :	<input type="text"/>	
MSN ACCOUNT :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
ICQ ACCOUNT :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
YAHOO ACCOUNT :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
QQ ACCOUNT :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
URL :	<input type="text"/>	
<input type="button" value="Search"/> <input type="button" value="Reset"/> <input type="button" value="Close"/>		

Item	Description	sample
BSSID	Mac address of access point	00:0E:2E:A3:7A:86
MAC	Mac address of computer	00:0E:2E:A3:7A:86
URL	Uniform Resource Locator.	www.yahoo.com.au

1. Example (by IP):

Searching all data belonged to IP [192.168.1.20], please input the IP in IP field. Press button [Search] to start searching.

The image shows a software interface for searching data. The top window is titled "Search Conditions" and contains a form with various search criteria. The "IP" field is pre-filled with "192.168.1.20". Below the form are "Search", "Reset", and "Close" buttons. A red arrow points from the "Search" button to a second window below. This second window displays a "MENU" of search results, including categories like POP3, SMTP, IMAP, FTP, MSN, ICQ, YAHOO, VOIP, HTTP, WEBMAIL, TELNET, QQ, and P2P. Several items in the menu are circled in red, and red arrows point from them to a yellow box on the right. A red text box on the right says "click one of these menus to get the findings".

SEARCH CONDITION		APPLY MODULE
DATE :		ALL
TIME :		
IP :	192.168.1.20	
BSSID :		
MAC :		
EMAIL :	<input type="checkbox"/> FROM <input type="checkbox"/> TO <input type="checkbox"/> CC <input type="checkbox"/> BCC	
SUBJECT :		
WEBMAIL TYPE :		
FTP SERVER IP :		
FTP ACCOUNT :		
MSN ACCOUNT :	1: 2: <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
ICQ ACCOUNT :	1: 2: <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
YAHOO ACCOUNT :	1: 2: <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
QQ ACCOUNT :	1: 2: <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
URL :		
<input type="button" value="Search"/> <input type="button" value="Reset"/> <input type="button" value="Close"/>		

MENU

Hard Disk Information : - 9.8G / Used - 7.9G / Available - 61G / Available (%) - 88%

- POP3 (0)
- SMTP (0)
- IMAP (0)
- FTP (0)
- MSN (24)
- ICQ (1)
- YAHOO (1)
- VOIP (0)
- HTTP (424)
- HTTP (DYNAMIC) (167)
- WEBMAIL (11)
- WEBMAIL (SENDING)
- TELNET (2)
- QQ (0)
- P2P (0)

click one of these menus to get the findings

1. Example (by IP & MSN)

Two inputs in different fields [ex. IP = 192.168.1.20 and MSN = she0430@hotmail.com].

To find out the information belonged to IP address 192.168.1.20 or MSN account she0430@hotmail.com

The image shows a web application interface for searching information. The top section is titled "Search Conditions" and contains a form with various input fields. The "IP" field is filled with "192.168.1.20" and the "MSN ACCOUNT" field is filled with "she0430@hotmail.com". The "APPLY MODULE" column on the right shows "ALL" for the IP field and a person icon for the MSN field. Below the form are "Search", "Reset", and "Close" buttons. A red arrow points from the "Search" button to the "MENU" section of the application. The "MENU" section is located at the bottom left and contains a list of services: POP3 (0), SMTP (0), IMAP (0), FTP (0), and MSN (24). The "MSN (24)" item is circled in red. A red arrow points from the "MSN (24)" item to the text "click msn to get the findings". At the top of the menu, there is a status bar that reads "Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%".

SEARCH CONDITION		APPLY MODULE
DATE :		
TIME :		
IP :	192.168.1.20	ALL
BSSID :		
MAC :		
EMAIL :	<input type="checkbox"/> FROM <input type="checkbox"/> TO <input type="checkbox"/> CC <input type="checkbox"/> BCC	
SUBJECT :		
WEBMAIL TYPE :		
FTP SERVER IP :		
FTP ACCOUNT :		
MSN ACCOUNT :	1 she0430@hotmail.com 2 <input checked="" type="checkbox"/> SCREEN NAME <input checked="" type="checkbox"/> PARTICIPANTS	
ICQ ACCOUNT :	1 2 <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
YAHOO ACCOUNT :	1 2 <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
QQ ACCOUNT :	1 2 <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
URL :		

Search Reset Close

MENU

- POP3 (0)
- SMTP (0)
- IMAP (0)
- FTP (0)
- MSN (24)**

Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%

click msn to get the findings

2. Special Search Type [only apply to MSN / ICQ / YAHOO]

Example 1: input one account in **MSN / ICQ / YAHOO** user's ID (monitor end) and **Chatter's ID** (remote end).

The screenshot shows a web-based search interface. At the top, there are input fields for FTP ACCOUNT, MSN ACCOUNT (with two sub-entries), ICQ ACCOUNT (with two sub-entries), YAHOO ACCOUNT (with two sub-entries), and QQ ACCOUNT (with two sub-entries). Each account type has checkboxes for 'SCREEN NAME' and 'PARTICIPANTS'. A 'URL' field is at the bottom left. A 'Search' button is at the bottom right. Red arrow 1 points to the 'Search' button. Below the search form, there is a 'MENU' on the left with options: POP3 (0), SMTP (0), IMAP (0), FTP (0), and MSN (1). Red arrow 2 points to the 'MSN (1)' menu item. To the right of the menu, there is a 'Hard Disk Information' bar showing - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%. Below the menu, there is a table titled 'CONDITION: MSN - 10.5.32.49'. Red arrow 3 points to the table. The table has columns: NO., DATE / TIME, SCREEN NAME, PARTICIPANTS, CONVERSATION, and COUNTS. It contains one row of data. At the bottom of the table, it says 'Count: 1, Total: 1, In page 1 | Rows per page: 20' and a 'Submit' button.

NO.	DATE / TIME	SCREEN NAME	PARTICIPANTS	CONVERSATION	COUNTS
1.	2007-04-11 11:10:24	alecwang@hotmail.com	liuyingshcn@hotmail.com	CONVERSATION	

Count: 1, Total: 1, In page 1 | Rows per page: 20






Here is the data searched by criteria, which both meet the criteria of **user's ID** [alecwang@hotmail.com] and **chatter's ID** [liuyingshcn@hotmail.com].

Hence, it can be categorized into two combinations:

1. User's nickname is [alecwang@hotmail.com] and chatter's ID is [liuyingshcn@hotmail.com].
2. User's nickname is [liuyingshcn@hotmail.com] and chatter's nickname is [alecwang@hotmail.com].

Example 2:

Input more than one IDs on the one blank field shown as following:

MSN ACCOUNT :	1.	cch926e@hotmail.com ; diesis@ms62.hinet.net ; liupeng19820923@hotmail.com	
	2.	she0430@hotmail.com	
		<input checked="" type="checkbox"/> SCREEN NAME <input checked="" type="checkbox"/> PARTICIPANTS	
ICQ ACCOUNT :	1.		
	2.		
		<input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
YAHOO ACCOUNT :	1.		
	2.		
		<input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
QQ ACCOUNT :	1.		
	2.		
		<input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
URL :			  
<input type="button" value="Search"/> <input type="button" value="Reset"/> <input type="button" value="Close"/>			

Here is the searched data by criteria, that's the data user's ID [cch926e@hotmail.com OR diesis@ms62.hinet.net OR liupeng19820923@hotmail.com] AND chatter's ID [she0430@hotmail.com].



No.	日期 时间	使用者代碼	對話者代碼	記錄檔	筆數
1.	2004-10-16 10:21:00	cch926e@hotmail.com	she0430@hotmail.com	記錄檔	93
2.	2004-10-16 14:00:03	cch926e@hotmail.com	she0430@hotmail.com	記錄檔	24

共 2 筆, 共 1 頁, 目前在第 1 頁 | 每頁顯示: 10 |








Hence, it can be categorized into three combinations:

1. User's ID is [cch926e@hotmail.com] and chatter's ID is [she0430@hotmail.com].
2. User's ID is [diesis@ms62.hinet.net] and chatter's ID is [she0430@hotmail.com].
3. User's ID is [liupeng19820923@hotmail.com] and chatter's ID is [she0430@hotmail.com].

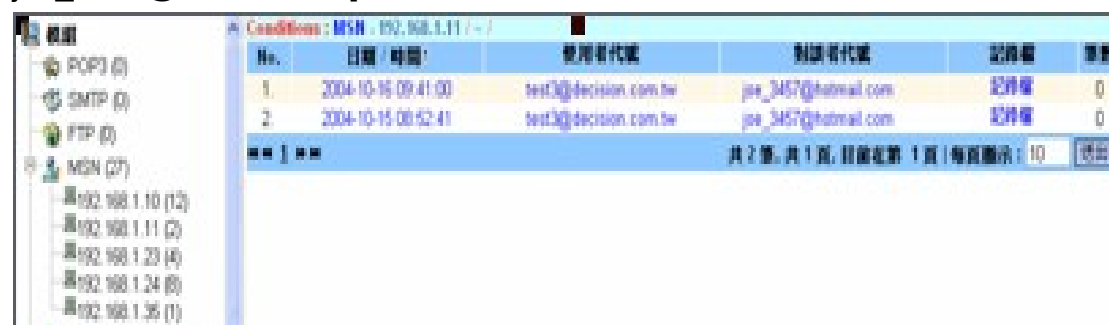
Copyright © 2007 Decision Computer International Co., Ltd

Example 3:

In **User's ID** of MSN / ICQ / YAHOO, input **two (or three) sets** of user's IDs and **don't input** chatter's ID, **you may check either User's ID (monitor end) or Chatter's ID (remote end), or both of them.**

MSN ACCOUNT :	1. bany1013@hotmail.com ; aries0724@msn.com ; joe_3457@hotmail.com 2. <input checked="" type="checkbox"/> SCREEN NAME <input checked="" type="checkbox"/> PARTICIPANTS	
ICQ ACCOUNT :	1. 2. <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
YAHOO ACCOUNT :	1. 2. <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
QQ ACCOUNT :	1. 2. <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
URL :	<input type="text"/>	  
<input type="button" value="Search"/> <input type="button" value="Reset"/> <input type="button" value="Close"/>		

Here is the searched data by criteria, that's the data of user's ID OR chatter's ID [bany1013@hotmail.com **OR** aries0724@msn.com **OR** joe_3457@hotmail.com].



No.	日期 / 时间	使用者代碼	對講者代碼	記錄檔	筆數
1.	2004-10-16 09:41:00	test3@decision.com.tw	joe_3457@hotmail.com	記錄檔	0
2.	2004-10-16 08:52:41	test3@decision.com.tw	joe_3457@hotmail.com	記錄檔	0





共 2 筆, 共 1 頁, 目前在第 1 頁 / 每頁顯示: 10

Hence, it can be categorized into six combinations:

1. User's ID is [bany1013@hotmail.com] and **any** chatter's ID.
2. User's ID is [aries0724@msn.com] and **any** chatter's ID.
3. User's ID is [joe_3457@hotmail.com] and **any** chatter's ID.
4. **Any** user's ID and chatter's ID is [bany1013@hotmail.com].
5. **Any** user's ID and chatter's ID is [aries0724@msn.com].
6. **Any** user's ID and chatter's ID is [joe_3457@hotmail.com].

Example 4:

In **User's ID** of MSN / ICQ / YAHOO, input **one set** of user's ID and **don't input** chatter's ID, **you may check either User's ID (monitor end) or Chatter's ID (remote end), or both of them.**

MSN ACCOUNT :	1. she0430@hotmail.com	
	2.	
<input checked="" type="checkbox"/> SCREEN NAME <input checked="" type="checkbox"/> PARTICIPANTS		
ICQ ACCOUNT :	1.	
	2.	
<input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS		
YAHOO ACCOUNT :	1.	
	2.	
<input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS		
QQ ACCOUNT :	1.	
	2.	
<input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS		
URL :		  
<div>Search Reset Close</div>		

Here is the searched data by criteria, that's the data of user's ID **OR** chatter's ID [she0430@hotmail.com].



No.	日期 / 时间	登录者代码	对话者代码	记录数	操作
1.	2004-10-14 17:00:46	test3@decision.com.tw	she0430@hotmail.com	12种	0

共 1 筆, 共 1 頁, 目前在第 1 頁 / 每頁顯示: 10 笔

Hence, it can be categorized into two combinations:

1. User's ID is [she0430@hotmail.com] and **any** chatter's ID.
2. **Any** user's ID and chatter's ID is [she0430@hotmail.com].

J. ALARM

E-Detective system allows administrator to set warning policy. Once data meets the criteria of warning policy after setting up, the system will send a warning mail to the mailbox of pre-defined **Receiving notification account** to provide administrator with instant information. If there is data which meets warning policy before setting up policy, it will not display the data whose date / time is prior to the date of setting up warning policy. When click on **Result**, it will display the items on the MENU which has met the policy set. Administrator can also click on **Search** to search all data defined warning policy.

The policy can include: source IP, subject, Web Mail Server, FTP Server IP, FTP account, MSN account, ICQ account, YAHOO account, URL etc. You may set up multiple criteria.

Warning includes numbering [No.], date, time, policy, viewing results and search.

The system provides an advanced warning function, you may search warning by predefined criteria.

Click the link [ALARM] to display following screen.

MENU

- POP3 (117)
- SMTP (46)
- IMAP (4)
- FTP (19)
- MSN (571)
- ICQ (2)
- YAHOO (2)
- VOIP (5)
- HTTP (25828)
- HTTP (DYNAMIC) (488)
- WEBMAIL (308)
- WEBMAIL (SENDER)
- TELNET (12)
- QQ (3)
- P2P (6)
- SEARCH
- ALARM**

Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%

NO.	DATE / TIME	RULE	RESULT	SEARCH
Count : 0 , Total : 0 , In page 0 Rows per page : 20				

[Create](#) [Renew](#) [Close](#) [Submit](#)

Click the button [Create] to display following screen; you may input criteria to match warning policy.

SEARCH CONDITION		APPLY MODULE
IP :	<input type="text"/>	ALL
BSSID :	<input type="text"/>	
MAC :	<input type="text"/>	
EMAIL :	<input type="text"/> <input type="checkbox"/> FROM <input type="checkbox"/> TO <input type="checkbox"/> CC <input type="checkbox"/> BCC	
SUBJECT :	<input type="text"/>	
WEBMAIL TYPE :	<input type="text"/>	
FTP SERVER IP :	<input type="text"/>	
FTP ACCOUNT :	<input type="text"/>	
MSN ACCOUNT :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
ICQ ACCOUNT :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
YAHOO ACCOUNT :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
QQ ACCOUNT :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> SCREEN NAME <input type="checkbox"/> PARTICIPANTS	
URL :	<input type="text"/>	
INFROM :	<input type="text"/>	
FORWARD :	<input type="text"/>	
<input type="button" value="Submit"/> <input type="button" value="Close"/>		

Item	Description	sample
BSSID	Mac address of access point	00:0E:2E:A3:7A:86
MAC	Mac address of computer	00:0E:2E:A3:7A:86
URL	Uniform Resource Locator.	www.yahoo.com.au
INFORM	Email account at where to send the warning.	admin@yahoo.com
FORWARD	Email account at where to send the warning.	admin@hotmail.com

Example: Input IP address "192.168.1.20" on the IP field and service@decision.com.tw" on the INFORM field. Press the button [submit]. The new rule is generated shown as the following:.

Hard Disk Information : - 736 / Used - 7.96 / Available - 616 / Available (%) - 88%

NO.	DATE / TIME	RULE	RESULT	SEARCH
6.	2007-04-26 12:00:42	RULE	RESULT	

Count : 1, Total : 1, In page 1 | Rows per page : 20

delete

Starting this rule right now otherwise it will be activated in 2 hours.

To see the rule content

Findings appeared here

Searching function

MENU

- POP3 (117)
- SMTP (46)
- IMAP (4)
- FTP (19)
- MSN (571)
- ICQ (2)
- YAHOO (2)
- VOIP (5)
- HTTP (25828)
- HTTP (DYNAMIC) (4887)
- WEBMAIL (308)
- WEBMAIL (SENDER) (97)
- TELNET (12)
- QQ (3)
- P2P (6)

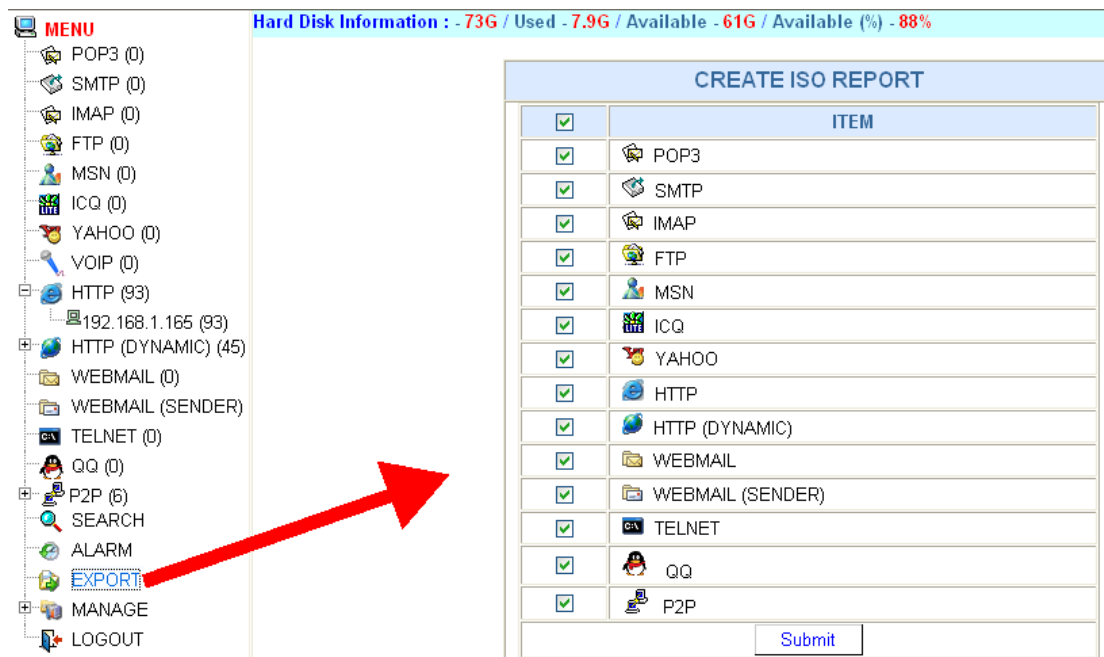
Renew

The alarming setup will renew in every hour time. When administrator would like to View the **Result**, it is advised to click on the **Renew** button to update the system.

K. Export

ED system provides export function to export the data to HD or CD. User selects what data type the ED system exports the data.

Click the link [EXPORT] to display following screen.

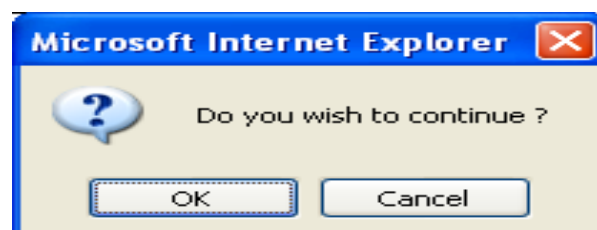


The screenshot shows the ED system interface. On the left is a 'MENU' sidebar with various options. A red arrow points from the 'EXPORT' option in the menu to the 'CREATE ISO REPORT' dialog box on the right. The dialog box has a title bar 'CREATE ISO REPORT' and a table with columns 'ITEM' and a checkbox. All items in the table are checked. A 'Submit' button is at the bottom right of the dialog box.

<input checked="" type="checkbox"/>	ITEM
<input checked="" type="checkbox"/>	POP3
<input checked="" type="checkbox"/>	SMTP
<input checked="" type="checkbox"/>	IMAP
<input checked="" type="checkbox"/>	FTP
<input checked="" type="checkbox"/>	MSN
<input checked="" type="checkbox"/>	ICQ
<input checked="" type="checkbox"/>	YAHOO
<input checked="" type="checkbox"/>	HTTP
<input checked="" type="checkbox"/>	HTTP (DYNAMIC)
<input checked="" type="checkbox"/>	WEBMAIL
<input checked="" type="checkbox"/>	WEBMAIL (SENDER)
<input checked="" type="checkbox"/>	TELNET
<input checked="" type="checkbox"/>	QQ
<input checked="" type="checkbox"/>	P2P

Submit

Press the button [Submit] to display following screen



Press [OK] button and start generating the ISO file shown as following:

35%
start

Once the process's done, the following window is popped up.

Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%

(Make ISO) Backup Rawdata & Unknown iso file size : 600 MB

PATH : /datas/rawdata

Rawdata File Name :

WIRELESS_00:0D:88:44:E7:F3_raw.1170240167 -- 56K
WIRELESS_00:0D:88:44:E7:F3_raw.1170332209 -- 60K
WIRELESS_00:11:95:DA:25:13_raw.1170405737 -- 601M
WIRELESS_00:11:95:DA:25:13_raw.1170406098 -- 184M
WIRELESS_00:11:95:DA:25:13_raw.1170425212 -- 2.7M
WIRELESS_00:11:95:DA:25:13_raw.1170426255 -- 1.9M
WIRELESS_00:11:95:DA:25:13_raw.1170426525 -- 1.3M
WIRELESS_00:11:95:DA:25:13_raw.1170426781 -- 7.9M

Submit Delete

PATH : /datas/fault

Raw File Name :

UNKNOWN_WIRELESS_00:0D:88:44:E7:F3_raw.1170332209 -- 8.0K
UNKNOWN_VOIP_WIRELESS_00_12_0E_21_19_75_raw.1161370826 -- 7.6M
UNKNOWN_QQ_WIRELESS_00_0F_A3_2A_08_44_raw.1162810224 -- 252K
UNKNOWN_MAP_WIRELESS_00_12_0E_21_19_75_raw.1161350816 -- 20K
UNKNOWN_WIRELESS_00:0D:88:44:E7:F3_raw.1170240167 -- 56K
UNKNOWN_WIRELESS_00:0D:88:44:E7:F3_raw.1170332209 -- 60K
UNKNOWN_WIRELESS_00:11:95:DA:25:13_raw.1170405737 -- 601M
UNKNOWN_WIRELESS_00:11:95:DA:25:13_raw.1170406098 -- 184M
UNKNOWN_WIRELESS_00:11:95:DA:25:13_raw.1170425212 -- 2.7M
UNKNOWN_WIRELESS_00:11:95:DA:25:13_raw.1170426255 -- 1.9M
UNKNOWN_WIRELESS_00:11:95:DA:25:13_raw.1170426525 -- 1.3M
UNKNOWN_WIRELESS_00:11:95:DA:25:13_raw.1170426781 -- 7.9M

Submit

(Burn ISO) Burn Rawdata Iso File, Burn Query File, Burn Iso File

Iso File Name : backcd_1.iso -- 2.9M DVD/CDROM : Burn CD Delete

ISO file will be appeared here

select the device to backup

save file to HD

Note: Exporting function can only export the data on the left of function menu; the default is to export all data. For example, you've searched all data of IP = 192.168.1.20 and their results are displayed on the left of function menu, then exporting data is all data of IP = 192.168.1.20 not that all of IP.

L. Wireless

Wireless Network Management

1. Proactive Crack and Passive Crack

Wireless Detective provides 2 options of crack function on the user interface: Proactive Crack and Passive Crack:

(1)Proactive Crack

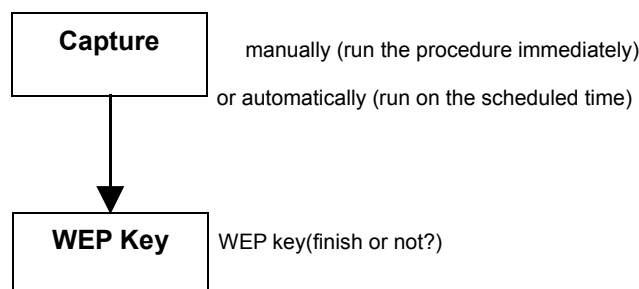
Proactive Crack means to crack by system automatically; i.e. The system proactively runs both of the capture and crack procedure at the same time, when the system starts capturing data. Decision Computer-“Wireless Detective” provides the function of proactive crack on the sub-menu(tab) of “CAPTURE”. Proactive crack runs the “ **capture and crack procedure** ” simultaneously. When the crack procedure completes, the system then runs the (recover, revert, restore, return) procedure to (revert, decrypt) the data.

(2)Passive Crack

Passive Crack means to crack by users manually. System passively runs the capture procedure only, without the crack procedure. Then it runs the crack function manually as needed. Decision Computer-“Wireless Detective” provides the function of “Passive Crack” on the sub-menu (tab) of “IMPORT”. Passive crack includes the following steps: (1)select the source of raw data, (2)set the time to use for crack procedure, (3)complete the crack procedure within the time interval.

2. Proactive Crack and Passive Crack: process chart

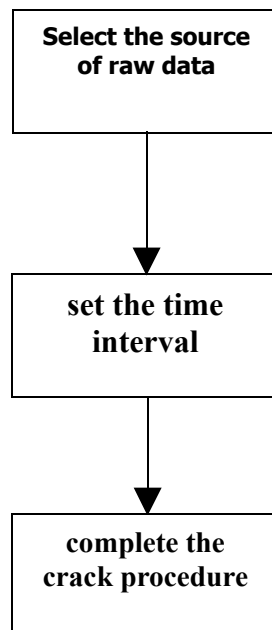
(1) Proactive Crack



※Please refer p.43 "Capture" for more detail

Copyright © 2007 Decision Computer International Co., Ltd

(2) Passive Crack



※Please refer p.49 "Import" for more detail

WEP Cracking Measurement Report

64 bits WEP Key Cracking Report				
Type of Key	Time	Packets (x1000)	IVS	ARP Packets
Numerical	10m36s	16,488	24,664	29,600
Alphabetical	18m25s	41,552	51,016	86,754
Num + Alpha	11m04s	25,380	32,990	56,513

128 bits WEP Key Cracking Report				
Type of Key	Time	Packets (x1000)	IVS	ARP Packets
Numerical	15m10s	27,804	41,919	62,073
Alphabetical	15m26s	31,532	44,183	58,624
Num + Alpha	17m10s	17,772	33,355	15,896

Wireless setup MENU involves six sub-menus: Capture, Import, Wepkey, History, Work Log, Ids.

1. Capture

Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%

Capture Import Wepkey History Work Log Ids

MODE : ☒ AP ☐ STA

Capture Size : 10096 K In Time Condition Dump Filter Condition Save List Refresh: 7 s. START STOP

By Channel

1 START START

By Channel + Ap

AP	SCAN	MANUAL DUMP	AUTO DUMP	BSSID	CH	MB/S	WEPKEY	STR	BEA	PACKETS	ESSID	STA
1	<input type="radio"/>	START	START	# 00:0D:88:44:E7:F3	7	11	WEP	34	21120	2122	meeting	0
2	<input type="radio"/>			# 00:0F:3D:33:29:F7	6	54	WEP?	10	4470	0	sung	0
3	<input type="radio"/>	START	START	# 00:11:95:DA:25:13	5	54	OPN	68	14961	10880	Dlink_abg	5
4	<input type="radio"/>	START	START	# 00:13:46:F0:87:B3	6	54	WPA	13	9498	129	DG_KC-Home	0
5	<input type="radio"/>	START	START	# 00:17:D1:FE:F3:F0	4	54	OPN	0	40	0	WIFLY	0
6	<input type="radio"/>	START	START	# 00:17:D1:FF:07:60	10	36	OPN	2	2080	22	WIFLY	2
7	<input type="radio"/>			# 00:17:D1:FF:07:61	10	54	WEP?	2	1510	0		0
8	<input type="radio"/>	START	START	# 00:17:D1:FF:07:62	10	54	OPN	3	1521	0		0
9	<input type="radio"/>	START	START	# 00:17:D1:FF:07:63	10	54	OPN	3	1467	0		0

Count : 9 , Total : 1 , In page 1 | Rows per page : 20 Submit

Features in this user interface (UI):

[1] : **MODE** : ☒ **AP** ☐ **STA** : Selecting access point (AP) or Wireless enabled PC (STA) to be target for capturing the information from.

[2] : **Capture Size** : 10096 **K** : Displaying the wireless transmitted data size in Kbyte.

[3] : **In Time Condition** : A filter to alarm the particular information or target based on specific conditions.

[4] : **Dump Filter Condition** : A filter to alarm the particular target based on specific conditions.

Copyright © 2007 Decision Computer International Co., Ltd

[5] : **Save List** : To save all access points and PCs scanned into the history page.

[6] : **Refresh:** s. **START STOP** : Refresh the information per specific seconds. Click links [START] or [STOP] to operate this function.

By Channel

[7] : : Set up which channel on access point to capture the information from.

[8] : : The right button means manually starting the capturing after pressing this button. The left button means auto-starting the capturing at the specific time.

[9] : **AP** : A function to mark access points with symbol @. To remind users when those access points marked are online.

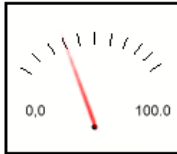
SCAN

[10] : ☐ : Showing the signal strength of access points and PCs.

Wireless Signal Detect Screen

REFRESH : TIME: s.

MODE	BSSID
<input type="text" value="AP"/>	<input type="text" value="00:15:E9:5D:AE:13"/>



STRENGTH : 30
SIGNAL : -95 dbm

[11] : : Two links present the exactly same user interface.

Set up the way to operate the ED system. Left one is for operating manually, another is for auto-operating. More detail is introduced later.

[12] : **#** : Showing Nic card's information.

Nic Info.

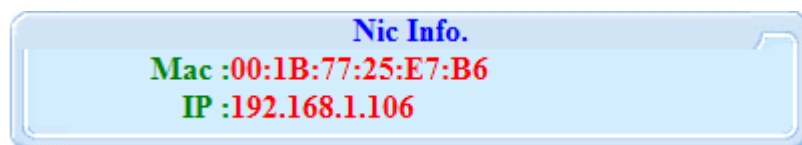
Mac : 00:02:2D:B8:60:49
Company : Agere Systems
P.O. Box 755
Information : 3430 At Nieuwegein
The Netherlands
NETHERLANDS

- [13] : **BSSID** : The Mac address of access point.
- [14] : **CH** : The channel number of access point.
- [15] : **MB/S** : Data transfer rate.
- [16] : **STR** : The signal strength.
- [17] : **BEA** : Information packed by BEA format for wireless transfer.
- [18] : **PACKETS** : The number of packets transferred.
- [19] : **ESSID** : The readable name of mac address for access point.
- [20] : **STA** : Display the PCs' information by number of PC scanned or radio.
- [21] : **WEP** : One of security keys used to transfer information.
- [22] : **WEP?** : The security key goes with question mark means the system has not yet collected any packets from the Wireless AP/Sta.
- [23] : **OPN** : Means there is no security key involved in this packet.

Capture Import Wepkey History Work Log Ids										
MODE : <input type="radio"/> AP <input checked="" type="radio"/> STA										
Capture Size : 10096 K In Time Condition Dump Filter Condition Save List Refresh: 7 s. START STOP										
STA	SCAN	MANUAL DUMP	AUTO DUMP	CLIENT MAC	STR.	PACKETS	BSSID	WEPKEY	CH.	ESSID
1	<input type="radio"/>	START	START	# ip 00:05:4E:42:DE:E2	29	1572	00:11:95:DA:25:13	OPN	5	Dlink_abg
2	<input type="radio"/>			# ip 00:05:4E:43:40:CA	0	34	00:11:95:40:40:AF	WEP?	6	JasonCo
3	<input type="radio"/>	START	START	# ip 00:0E:2E:A3:7A:86	-1	13	00:17:D1:FF:07:60	OPN	10	WIFLY
4	<input type="radio"/>			# ip 00:0E:35:52:8F:5A	1	13	FF:FF:FF:FF:FF:FF			
5	<input type="radio"/>	START	START	# ip 00:0E:35:87:21:14	35	3401	00:11:95:DA:25:13	OPN	5	Dlink_abg
6	<input type="radio"/>	START	START	# ip 00:0E:35:8E:3D:B9	47	9261	00:11:95:DA:25:13	OPN	5	Dlink_abg
7	<input type="radio"/>	START	START	# ip 00:0E:35:96:61:E8	59	6556	00:11:95:DA:25:13	OPN	5	Dlink_abg
8	<input type="radio"/>	START	START	# ip 00:0E:35:E4:77:F9	-1	9	00:17:D1:FF:07:60	OPN	10	WIFLY
9	<input type="radio"/>	START	START	# ip 00:20:A6:58:86:A7	41	170	00:11:95:DA:25:13	OPN	5	Dlink_abg
Count : 9 , Total : 1 , In page 1 Rows per page : 20 Submit										

Features in this user interface (UI):

- [1] : **ip** : A link to show the information of Mac address of PC and IP.



- [2] : Others are already introduced on the AP's UI. Please refer there to see more detail.

Copyright © 2007 Decision Computer International Co., Ltd

Decrypt Information manually: [WEP](#) [WEP?](#) [WPA](#)

Click these three links appeared on the table will pop up the following windows is able to get the security key from user's input in order to decrypt the information manually.



The image shows a web-based dialog box titled "Edit Wepkey". It contains a text input field for entering a key. To the right of the input field is a dropdown menu currently set to "ASCII". Below the dropdown, the options "HEX" and "ASCII" are visible. To the right of the dropdown are two buttons: "Submit" and "Close".

Note:

HEX is from 0-10 and A-F or a-f

ASCII defines codes for 128 characters: 33 are non-printing, mostly obsolete control characters that affect how text is processed, and 95 are printable characters.

In Time Condition: [In Time Condition](#)

User specifies the conditions below and presses the start button to start this filter. The filter alerts user by popping up a message when there is any incoming data corresponds or matches the conditions specified here.

In Time Scan Condition Setup

STATUS : stop

Condition Item Set				Condition List
CHANNEL :	1	<input type="button" value="v"/>	<input type="button" value=">>"/>	<div></div> <div>Delete</div>
IP :	<input type="text"/>		<input type="button" value=">>"/>	
MAC :	<input type="text"/>		<input type="button" value=">>"/>	
NETWORK :	<input type="text"/>		<input type="button" value=">>"/>	
KEYWORD	HEX :	<input type="text"/>	<input type="button" value=">>"/>	
	STRING :	<input type="text"/> Big5 <input type="button" value="v"/>		
<div>Start</div>				

Dump Filter Condition: [Dump Filter Condition](#)

User specifies the conditions shown as the following diagram to only capture the information from the particular targets.

Dump Filter Condition Setup

Condition Item Set			Condition List
IP :	<input type="text"/>	<input type="button" value=">>"/>	<div></div> <div>Delete</div>
MAC :	<input type="text"/>	<input type="button" value=">>"/>	
NETWORK :	<input type="text"/>	<input type="button" value=">>"/>	
<div>Submit</div>			

MANUAL DUMP & AUTO DUMP: [MANUAL DUMP](#) [AUTO DUMP](#)

1. Set up which Nic card to scan or manage/Dump information.

Wireless Nic Setup	
Scan :	wifi1 ▼
Dump :	wifi0 ▼
Submit	
Remark : On Board : wifi0 Pcmcia : wifi1	

2. How long to attack targets for obtaining the security key and whether use this function or not.

Wireless Inject Setup	
Speed :	20 ▼ ms.
Submit	
Use ? :	<input checked="" type="radio"/> Yes <input type="radio"/> No
Submit	

3. Set up the max size per file for backup.

Wireless Rawdata file Size Setup	
Size :	600 ▼ mb.
Submit	
Remark : Rawdata file size default is 600 MB.	

4. To alarm user when HD usage exceeds the threshold specified.

Upper limit of Hard Disk Size Setup	
Percent :	80 %
Submit	

5. Set up how long to refresh the information scanned.

Scan Info. Refresh Time Setup	
Time :	5 ▼ m.
Submit	

System is capable to start the wireless packet capturing and decoding process manually by user or automatically by pre-setup/ configuration.

Figure below shows the configuration to be done for auto start capturing at defined data and time.

自動收集時間設定	
對象 :	AP
BSSID :	00:00:00:00:00:00
CLIENT MAC :	
ESSID :	
頻道 :	07
金鑰 :	OPN
設定狀況 :	START
開始時間 :	2007-07-01  01  : 59 
結束時間 :	2007-07-31  23  : 59 
<input type="button" value="呈送"/>	

2. Import

This function imports captured information (raw data in tcp dump format) to the system for decoding purpose. There are four sources of raw data to choose: CD-ROM, USB drive, HD and DETACH. DETACH contains the currently captured raw data in Wireless E-Detective system.

Press the button [Read File], the system displays the raw data information and lists it on the table. By selecting the particular AP or Station, user can crack the encryption key (WEP and WPA) if the collecting raw data is sufficient (about 100-150MB for 64-bit WEP key and 250-400MB for 128-bit WEP key). Cracking WPA key is a customizable option the Decision Computer Int' Co., Ltd can offer. For WPA, the first key must be obtained in order to crack the key.

After cracking the key, user ticks the radio on the PARSER column to decode the captured data and display it in readable format according to specific groups in the MENU. If there is no radio on the CRACK column, user directly clicks the radio on the PARSER column to decode the captured raw data without needing to crack any encryption. If user knows the WEP or WPA key in advance, user can click on the [WEP](#) or [WPA](#) key and input the key.

The screenshot shows the 'Import' tab of the Wireless E-Detective software. The interface includes a left sidebar with a menu of various protocols and services. The main window displays a 'Please Choose Rawdata Source' dialog box with options for CD-ROM, USB, HD, and DETACH. Below this, there is a 'Manual Wireless Packet Analysis' section with fields for 'Crack Time' and 'Crypt' (128 Bit). The main area contains two tables of captured data.

Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%

Please Choose Rawdata Source

RAWDATA SOURCE : DETACH PATH : /datas/openraw

☐ CD-ROM ☐ USB ☐ HD ☒ DETACH

WIRELESS_00:11:95:DA:25:13_raw.1177580030-9.9M

Manual Wireless Packet Analysis

Crack Time : 1 m. Crypt : 128 Bit

Finish !

AP	PARSER	CRACK	BSSID	CH.	MB/S	WEPKEY	BEACONS	PACKETS	ESSID
1	<input type="radio"/>		00:0A:79:98:1C:A5	6	54	OPN	2	0	corega
2	<input type="radio"/>	<input type="radio"/>	00:0D:88:44:E7:F3	7	11	WEP	2440	208	meeting
3	<input type="radio"/>		00:11:95:DA:25:13	5	54	OPN	5443	28477	Dlink_abg
4	<input type="radio"/>		00:13:46:F0:87:B3	6	54	WPA	1986	25	DG_KC-Home

STA	PARSER	CRACK	CLIENT MAC	PACKETS	BSSID	CH.	WEPKEY	ESSID
1	<input type="radio"/>		00:0E:35:87:21:14	361	00:11:95:DA:25:13	5	OPN	Dlink_abg
2	<input type="radio"/>		00:0E:35:8E:3D:B9	5026	00:11:95:DA:25:13	5	OPN	Dlink_abg
3	<input type="radio"/>		00:0E:35:96:61:E8	23948	00:11:95:DA:25:13	5	OPN	Dlink_abg
4	<input type="radio"/>		00:0E:35:BA:09:2B	14	FF:FF:FF:FF:FF:FF			
5	<input type="radio"/>		00:20:A6:58:86:A7	31	00:11:95:DA:25:13	5	OPN	Dlink_abg

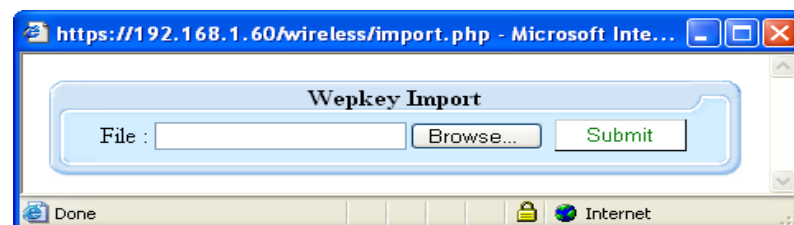
3. WEP key

This function shows the WEP key that has been cracked or imported. Besides, it allows user to import (from Excel file) and export (to Excel file) WEP key. It allows users to search through the wireless system for specific WEP key as well. Besides, it allows user to delete it from the list on this page.

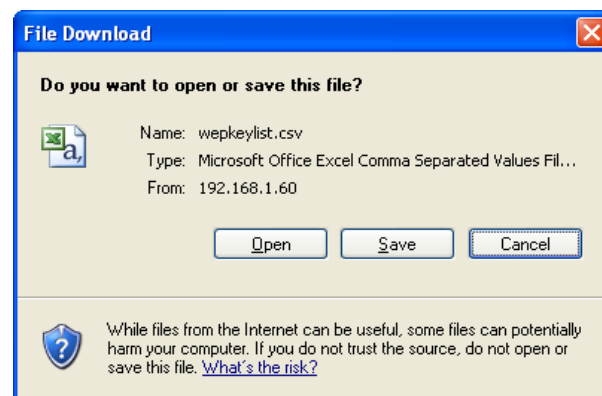
Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%

Capture	Import	Wepkey	History	Work Log	Ids
Delete	Import	Export	Search		
NO.	DATE / TIME↑	BSSID	WEPKEY		
No Data !					
Count : 0 , Total : 0 , In page 0 Rows per page : 20					
Submit					

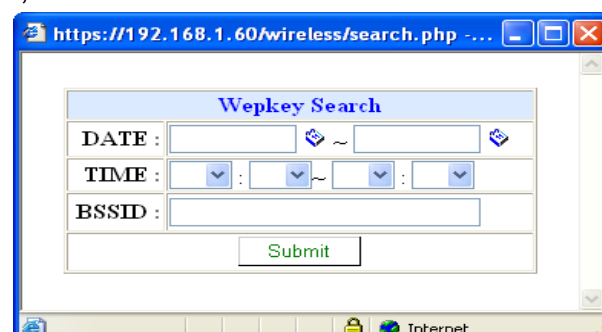
To import WEP key,



To export WEP key,



WEP key search,




4. History

This function shows the history of recorded APs and Stations and their respective details information such as BSSID, channel, data rate, WEP key, signal strength, beacon and packets captured by Wireless E-Detective systems and ESSID that has been saved or backup according to time.

Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%

Capture / Import / Wepkey / **History** / Work Log / Ids

Backup Time : 2007-02-02 08:57:25 

finish !

AP	BSSID	CH.	MB/S	WEPKEY	STRENGTH	BEACONS	PACKETS	ESSID
1	00:0A:79:49:CD:00	6	11	WEP?	2	62	0	
2	00:0A:79:82:2F:D0	6	54	WEP	1	66	4	corega
3	00:0D:88:44:E7:F3	7	11	OPN	56	1040	617	meeting
4	00:0E:2E:7B:1F:E5	11	54	WEP?	3	19	0	home-wireless
5	00:0F:3D:33:29:F7	6	54	WEP?	8	18	0	sung
6	00:11:95:DA:25:13	5	54	WEP	41	1488	34016	Dlink_abg
7	00:13:46:F0:87:B3	6	54	WEP?	12	21	0	DG_KC-Home
8	00:E0:98:51:0F:06	11	11	WEP?	6	136	0	Untitled

STA	CLIENT MAC	STRENGTH	PACKETS	BSSID	CH.	ESSID
1	00:0E:35:29:99:0C	37	545	00:11:95:DA:25:13	5	Dlink_abg
2	00:15:00:4B:CB:EC	27	573	00:0D:88:44:E7:F3	7	meeting
3	00:16:01:18:0B:CE	45	35152	00:11:95:DA:25:13	5	Dlink_abg

5. Work Log

This function shows the work log which includes time, E-Detective system MAC, BSSID, ESSID, channel, encryption type, filter, type, query and details of the network.

Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%

Work Log

NO.	DATE / TIME	ED MAC	BSSID	ESSID	CH.	WEPKEY	FILTER	TYPE	QUERY DETAIL
1.	2007-04-26 09:44:27	00:16:D3:2A:1C:BE	00:11:95:DA:25:13	Dlink_abg	5	OPN		IMPORT	QUERY DETAIL
2.	2007-04-26 09:43:41	00:16:D3:2A:1C:BE	00:11:95:DA:25:13	Dlink_abg	5	OPN		IMPORT	QUERY DETAIL
3.	2007-04-26 09:33:52	00:16:D3:2A:1C:BE	00:11:95:DA:25:13	Dlink_abg	5	OPN		MANUAL	QUERY DETAIL
4.	2007-04-20 11:01:49		00:11:95:DA:25:13	Dlink_abg	5	OPN		MANUAL	QUERY DETAIL
5.	2007-04-18 13:07:49	00:16:D3:2A:1C:BE	00:ED:98:55:B1:66	Untitled	11	OPN		MANUAL	QUERY DETAIL
6.	2007-04-17 12:58:58	00:16:D3:2A:1C:BE	00:00:00:00:00:00		1	OPN		MANUAL	QUERY DETAIL
7.	2007-04-16 17:12:27	00:16:D3:2A:1C:BE	00:0A:79:AA:A3:DB	decision+test	6	OPN		MANUAL	QUERY DETAIL

MENU

- POP3 (0)
- SMTP (0)
- IMAP (0)
- FTP (0)
- MSN (0)
- ICQ (0)
- YAHOO (0)
- VOIP (0)
- HTTP (79)
- HTTP (DYNAMIC) (23)
- WEBMAIL (0)
- WEBMAIL (SENDER) (0)
- TELNET (0)
- QQ (0)
- P2P (3)

find out the data belonged to this work log

Show the type of transferred packet and the size.

START TIME	END TIME	FILENAME	TCP ANALYZER OTHER	TCP ANALYZER OTHER	UDP ANALYZER OTHER	UDP ANALYZER OTHER
2007-04-26 09:43:41	2007-04-26 09:44:27	datacapture\WIRELESS_00:11:95:DA:25:13_00:16:D3:2A:1C:BE	580	246435	70	70

Count: 1, Total: 1, In page 1 / Rows per page: 20

6. IDS (Intrusion Information)

Information to notify user if there is any illegal internet packets scanned.

Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%		
Capture / Import / Wepkey / History / Work Log / Ids		
NO.	DATETIME↑	MESSAGE
1.	2007-04-18 16:20:59	Broadcast on 00:12:F0:4B:23:14
2.	2007-04-18 16:20:59	Broadcast on 00:12:F0:4B:23:14
3.	2007-04-18 16:20:57	Broadcast on 00:12:F0:4B:23:14
4.	2007-04-18 16:20:57	Broadcast on 00:12:F0:4B:23:14
5.	2007-04-18 16:20:55	Broadcast on 00:12:F0:4B:23:14
6.	2007-04-18 16:20:55	Broadcast on 00:12:F0:4B:23:14
7.	2007-04-18 16:20:52	Broadcast on 00:0C:2F:00:23:A8
8.	2007-04-18 16:20:52	Broadcast on 00:0C:2F:00:23:A8
9.	2007-04-18 16:20:52	Suspicious client 00:12:F0:4B:23:14 - probing networks but never joining.
10.	2007-04-18 16:20:47	Suspicious traffic on 00:0C:2F:00:23:A8 Data traffic within 10 seconds of a disassociate.
11.	2007-04-18 16:20:46	Suspicious client 00:12:F0:BC:D8:EA - probing networks but never joining.
12.	2007-04-18 16:20:43	Suspicious client 00:C0:02:50:C8:99 - probing networks but never joining.
13.	2007-04-18 16:20:41	Suspicious client 00:90:96:BA:BB:54 - probing networks but never joining.
14.	2007-04-18 16:20:41	Suspicious traffic on 00:0C:2F:00:23:A8 Data traffic within 10 seconds of a disassociate.
15.	2007-04-18 16:20:37	Suspicious traffic on 00:0C:2F:00:23:A8 Data traffic within 10 seconds of a disassociate.
16.	2007-04-18 16:20:35	Suspicious client 00:90:96:BA:BB:54 - probing networks but never joining.
17.	2007-04-18 16:20:35	Suspicious traffic on 00:0F:3D:33:25:01 Data traffic within 10 seconds of a disassociate.
18.	2007-04-18 16:20:33	Suspicious client 00:11:22:33:44:55 - probing networks but never joining.
19.	2007-04-18 16:20:30	Suspicious client 00:19:D2:1B:31:48 - probing networks but never joining.
20.	2007-04-18 16:20:30	Suspicious traffic on 00:0C:2F:00:23:A8 Data traffic within 10 seconds of a disassociate.
<< 1 2 3 4 5 6 7 8 9 >>		Count : 10097 . Total : 505 . In page 1 Rows per page : 20 <input type="button" value="Submit"/>

M. Backup Data

Backup data is divided into two parts:

- Backup raw data (ISO)
- Back up the list of Database log file

1. Backup Raw Data (ISO)

Use this function to selectively back up data. It consists of raw data, unknown data (unable to identify after parser) and created ISO file. User can select the file size of backup rawdata ISO file to create.

Step-by-step as follows:

1. Set up the Max size of each backup file.
2. Select the raw data file to convert to ISO format.
3. Press [Submit] to create ISO format. Press [Delete] to delete the raw data file.
4. The backup file is listed here when ISO file is generated.
5. Select the device to burn the data into CD.
6. Click this icon to save this backup into HD.
7. Press the button [Burn CD] to start processing or [Delete] to delete the file.

Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%

Backup (Rawdata) Backup (Database)

STEP 1. (Make ISO) Backup Rawdata & Unknow iso file size : 600 MB 1

PATH : /datas/rawdata

Rawdata File Name :

- WIRELESS_00:0D:88:44:E7:F3_raw.1170240167 -- 56K
- WIRELESS_00:0D:88:44:E7:F3_raw.1170332209 -- 60K
- WIRELESS_00:11:95:DA:25:13_raw.1170405737 -- 601M
- WIRELESS_00:11:95:DA:25:13_raw.1170406098 -- 184M
- WIRELESS_00:11:95:DA:25:13_raw.1170425212 -- 2.7M
- WIRELESS_00:11:95:DA:25:13_raw.1170426255 -- 1.9M
- WIRELESS_00:11:95:DA:25:13_raw.1170426525 -- 1.3M
- WIRELESS_00:11:95:DA:25:13_raw.1170426781 -- 7.9M

Submit Delete

PATH : /datas/fault

Unknow File Name :

- UNKNOWN_WIRELESS_00:0D:88:44:E7:F3_raw.1170332209 -- 8.0K
- UNKNOWN_VOIP_WIRELESS_00_12_0E_21_19_75_raw.1161370826 -- 7.6M
- UNKNOWN_QQ_WIRELESS_00_0F_A3_2A_08_44_raw.1162810224 -- 252K
- UNKNOWN_IMAP_WIRELESS_00_12_0E_21_19_75_raw.1161350816 -- 20K
- UNKNOWN_WIRELESS_00:0D:88:44:E7:F3_raw.1170428080 -- 48K
- UNKNOWN_WIRELESS_00:0D:88:44:E7:F3_raw.1170428618 -- 96K
- UNKNOWN_WIRELESS_00:0D:88:44:E7:F3_raw.1170429059 -- 56K
- UNKNOWN_WIRELESS_00:0D:88:44:E7:F3_raw.1170430147 -- 8.0K

Submit Delete

STEP 2. (Burn ISO) Burn Rawdata Iso File Choice raw*.iso File, Burn Query Iso File Choice backcd_*.iso File

4 Iso File Name : backcd_1.iso -- 14M 5 DVD/CDROM : 6 7

Burn CD Delete

Copyright © 2007 Decision Computer International Co., Ltd


2. Backup (Database)

Backing up database table to prevent form database damage, you may restore database by backup of log file. The log file will be generated once everyday.

Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%

Backup (Rawdata)

Backup (Database)



DATABASE BACKUP FILE

No Data !

N. SYSTEM

This function is divided into four parts:

- Network setup
- HDD usage
- Server
- Set up System Time

1. Network Setup

In this page, E-Detective System provides several setup functions:

- Network setup

The following page allows changing IP, Net mask, broadcasting and gateway of E-Detective System, you may set up here. Also set up which operation mode such as ALL IN ONE, CAPTURE, and ANALYZER here.

The DNS address is also set up here.

Note: the system will require rebooting.

Note: set up a real IP and log in remotely for browsing and controlling.

Hard Disk Information : - 55G / Used - 2.8G / Available - 49G / Available (%) - 94%

Network Setup | Check HD | Services | Update System Time

Network Setting

Device List		
Device	Mode	IP
eth0	M	192.168.1.60/255.255.255.0/192.168.1.255/192.168.1.1

Note : Mode M = MANAGE S = SEND FILE R = RECEIVE FILE

Setup

DNS Setting

Configuration	Default Setting	New Setting
Primary	192.168.1.1	
Second	168.95.1.1	

Submit

ALL IN ONE Mode:

This selection is for normal single layer function. Only one network card interface, eth0 is used for capturing and decoding purpose. After configuring the Manage IP, Net mask, Broadcast and Gateway address, Press [Submit] to complete the setup.

https://192.168.1.60/sys-control/setip.php - Micro...

FUNCTION : ☒ ALL IN ONE ☐ CAPTURE ☐ ANALYZER

MANAGE

Device : eth0

IP : 192.168.1.60

Netmask : 255.255.255.0

Broadcast : 192.168.1.255

Gateway : 192.168.1.1

Submit

Done Internet

CAPTURE Mode: (Sender)

This setup is for double layer architecture (Sender and Receiver ends). CAPTURE is set at the sender end. Firstly, set the configuration for the MANAGE setup. Then, complete the SEND FILE configuration with the Analyzer IP as the Receiver end (Decoder) IP. Press [Submit] to complete the configuration.

The screenshot shows a web browser window with the address bar displaying `https://192.168.1.60/sys-control/setip.php`. The page content is as follows:

FUNCTION : ☐ ALL IN ONE ☒ CAPTURE ☐ ANALYZER

MANAGE

Device : <input type="text" value="eth0"/>	IP :	<input type="text" value="192.168.1.60"/>
	Netmask :	<input type="text" value="255.255.255.0"/>
	Broadcast :	<input type="text" value="192.168.1.255"/>
	Gateway :	<input type="text" value="192.168.1.1"/>

SEND FILE

Device : <input type="text" value="eth0"/>	IP :	<input type="text" value="192.168.1.60"/>
	Netmask :	<input type="text" value="255.255.255.0"/>
	Broadcast :	<input type="text" value="192.168.1.255"/>
	Gateway :	<input type="text" value="192.168.1.1"/>
	Analyzer IP :	<input type="text" value="192.168.1.80"/>

The browser's status bar at the bottom shows "Done" and "Internet".

ANALYZER Mode: (Receiver or Decoding End)

This setup is for double layer architecture (Sender and Receiver ends). ANALYZER is set at the receiver or decoding end. Firstly, set the configuration for the MANAGE setup. Then, complete the RECEIVER FILE configuration. Press [Submit] to complete the configuration

https://192.168.1.60/sys-control/setip.php - Microsof...

FUNCTION : ☐ ALL IN ONE ☐ CAPTURE ☒ ANALYZER

MANAGE

Device : eth0 ▼	IP :	192.168.1.80
	Netmask :	255.255.255.0
	Broadcast :	192.168.1.255
	Gateway :	192.168.1.1

RECEIVE FILE

Device : eth0 ▼	IP :	192.168.1.80
	Netmask :	255.255.255.0
	Broadcast :	192.168.1.255
	Gateway :	192.168.1.1

Submit

Done Internet

2. HDD Usage

The system displays HDD usage information which includes HDD capacity, used space, free space and ratio of free space. E-Detective System pops up a warning message when used space reaches at threshold.

Also, it generates a warning letter to notify specified personnel of spaces are running out and take necessary measures. Setup step-by-step as follows:

1. Upload the contents file: you may customize the contents of warning file, and press Upload to be standard warning letter.
2. Set up the policy of warning letter: set up receiver's e-mail address, topic and contents, then press **Submit** to activate settings. The system will automatically send warning letter once used space reaches at threshold.

The screenshot displays the E-Detective System interface. On the left is a vertical menu with various system management options. The main window is titled 'Hard Disk Information : - 55G / Used - 2.8G / Available - 49G / Available (%) - 94%'. Below the title bar are tabs for 'Network Setup', 'Check HD', 'Services', and 'Update System Time'. The 'Check HD' tab is active, showing two main sections: 'Hard Disk Information' and 'Warning Message Setup'.

Hard Disk Information

Size	Used	Available	Available (%)
55G	2.8G	49G	94%

Warning Message Setup

UpLoad Warning-message file

File :

File
sample.txt

Warning-mail Rule

Email Address :

Subject :

File :

Rule	Email Address	Subject	File
No Data !			

3. Server

The ED system consists of a set of components/Servers. The following UI allows user to **activate** / **deactivate** some of these servers for purpose of saving computer's resource.

Service	Status	Action
ssh	Start	<input type="button" value="Stop"/>
inetd	Start	<input type="button" value="Stop"/>
conver	Start	<input type="button" value="Stop"/>
OpenRaw	Stop	<input type="button" value="Start"/>
emailsub	Start	<input type="button" value="Stop"/>
parser	Start	<input type="button" value="Stop"/>
tomcat	Start	<input type="button" value="Stop"/>
WirelessScan	Start	<input type="button" value="Stop"/>
MotoCrack	Stop	
gpsd	Stop	<input type="button" value="Start"/>
ntp	Stop	<input type="button" value="Start"/>
wirelessids	Stop	<input type="button" value="Start"/>
wifi0	Stop	<input type="button" value="Start"/>
wifi1	Start	<input type="button" value="Stop"/>
FireWall	Start	<input type="button" value="Setup"/>

Service	Description
SSH	Carries out the far-end segment
Inetd	Carries out the functions of POP3, IMAP, and SMTP.
conver	Carries out the conversion of codes.
OpenRaw	Carries out capture.
emailsub	Carries out the conversion of subject name.
parser	Carries out the classification/management of information.
tomcat	Carries out the navigation.
WirelessScan	Carries out scanning information.
MotoCrack	Carries out the manual decryption.
gpsd	Carries out the function of GPS
ntp	Adjusting the system time.
wirelessids	Investigation of unusual internet packets.
wifi 0	NIC card.
wifi 1	NIC card.
FireWall	To activate/de-activate the function.

Function: Users can be able to specify what IPs can access into ED system.

FireWall:

It creates specific IP for allowing login to E-Detective System.

Firewall Setup

Create Allow IP :

Delete | Delete All

<input type="checkbox"/>	Allow IP
<input type="checkbox"/>	192.168.1.0/24

Port numbers provided for reference.

Service List		
Service	Status	Port
ftp	Open	21
ssh	Open	22
pop3	Open	110
rpcbi	Open	111
auth	Open	113
https	Open	443
u	Open	630
u	Open	640
mysql	Open	3306
ajp13	Open	8009

4. Set up System Time

Providing the function to adjust the system time shown as the following:

Hard Disk Information : - 55G / Used - 2.8G / Available - 49G / Available (%) - 94%

[Network Setup](#) / [Check HD](#) / [Services](#) / [Update System Time](#)

System Time Update													
Current System Time :	2006-12-18 18:37												
* Update System time :	<table><thead><tr><th>Year</th><th>Mon.</th><th>Day</th><th>Hour</th><th>Min.</th><th></th></tr></thead><tbody><tr><td>2006</td><td>12</td><td>18</td><td>18</td><td>37</td><td><input type="button" value="Submit"/></td></tr></tbody></table>	Year	Mon.	Day	Hour	Min.		2006	12	18	18	37	<input type="button" value="Submit"/>
Year	Mon.	Day	Hour	Min.									
2006	12	18	18	37	<input type="button" value="Submit"/>								
* Correct Time Zone :	+8 <input type="button" value="Submit"/>												

O. Network Users

List of network user is divided into three parts:

1. On-line IP information
2. List of logged-in users
3. Nbns

If you don't set up the list of network users, Wireless E-Detective will automatically search users and IPs on network, and then perform sniffing and monitoring. There is an upper limit on the number of sniffing computer (depends on purchasing specification). It might sniff unnecessary user's information if let the Wireless E-Detective automatically retrieve user and IP. Hence, the list of network users can help administrator to specify which computer should be sniffed by Wireless E-Detective. Also, it can help to set up computer and group name for convenient monitoring.

1. On-line IP information

At first, you need to add IP to display the IP to be retrieved and select group. You may edit user's IP, computer name, group and the user's current status to be displayed on screen by the first section "Create" and [Submit]. Different IP with PC Name can be created in different Group.

[Online IP Info.](#) [Login User List](#) [Nbns](#)

Create Submit

IP	PC NAME	Status	LAST TIME	GROUP
<input type="text"/>	<input type="text"/>			GROUP1-1

NO.	<input type="checkbox"/>		Status	IP ↑	PC NAME	LAST TIME	ISP	GROUP
1.	<input type="checkbox"/>			192.168.1.53	DDD			GROUP1
2.	<input type="checkbox"/>			192.168.1.52	CCC			GROUP1
3.	<input type="checkbox"/>			192.168.1.51	BBB			GROUP1
4.	<input type="checkbox"/>			192.168.1.50	AAA			GROUP1

Count : 4 , Total : 1 , In page 1 | Rows per page : 20 Submit

DeleteImportExportSkip IPSet IPAuto SearchISP

To add IP:

- Click **Auto search** to display following window. Input the IP segment to be searched and get IP of on-line computer; check the computer IP you want to add and click **Update** to add it.

Auto Search IP List			
VERSION : 10 / 65535			
<input type="checkbox"/>	User IP	PC Name	Group
<input type="checkbox"/>	192.168.1.18		GROUP1--1
<input checked="" type="checkbox"/>	192.168.1.6		GROUP1--1
<input type="checkbox"/>	192.168.1.1		GROUP1--1
<input checked="" type="checkbox"/>	192.168.1.2		GROUP1--1
<input type="checkbox"/>	192.168.1.15		GROUP1--1
<input checked="" type="checkbox"/>	192.168.1.17		GROUP1--1
<input type="checkbox"/>	192.168.1.5		GROUP1--1

- Click **Import** to display following window. You may edit an Excel file and upload it to system. Format: IP;MAC;NAME;GROUP [file type is *.CSV] [GROUP = 1] [MAC can be blank].

https://192.168.1.60/userlist/list.php - Microsoft Internet Expl...

Import File

File : Browse... Import

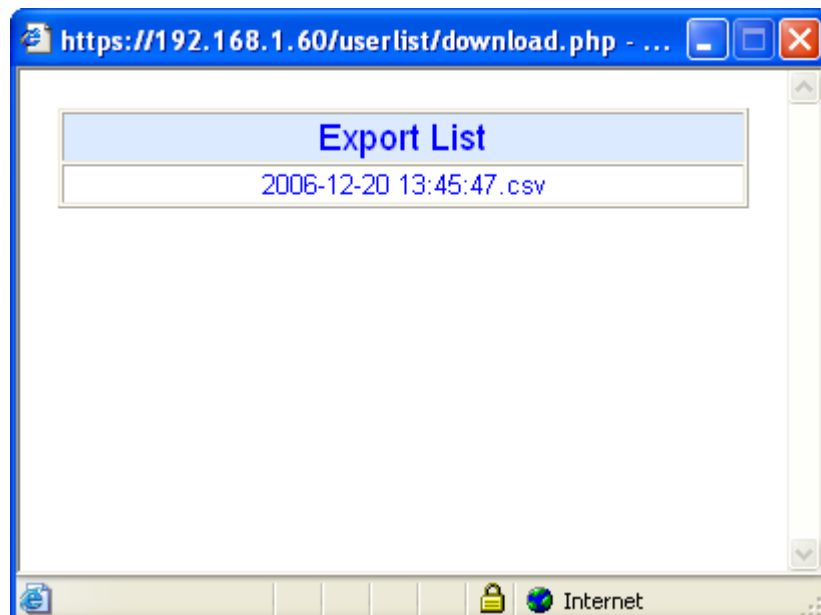
Close

Done Internet


Note: Name can't be Chinese character; if you need to input Chinese, please convert it to Unicode and upload. °

Note: Mac address is proprietary location of LAN adapter.

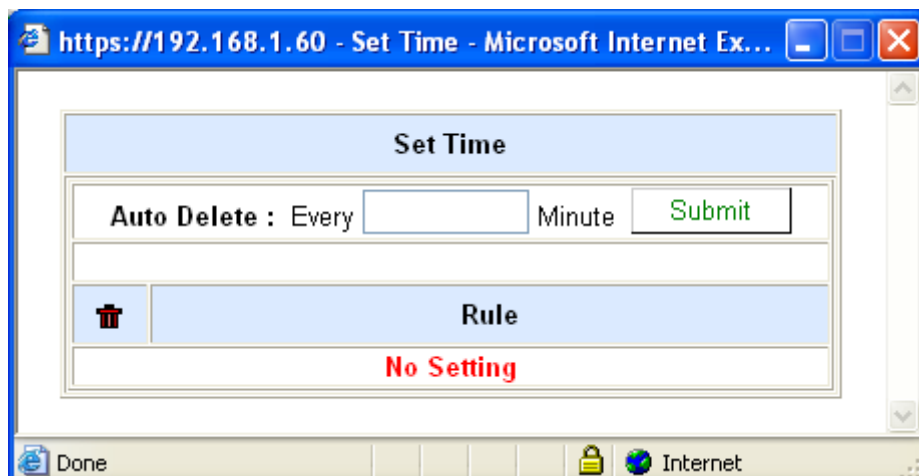
- Click **Export** to display following window. You may export IP list and back up.



- Click **Skip IP Setup** to display following window, and then set up the IP not to be sniffed.

Skip IP Setup			
IP :	<input type="text"/> <input type="button" value="Submit"/>		
	<table border="1"><thead><tr><th>IP</th></tr></thead><tbody><tr><td>No Data !</td></tr></tbody></table>	IP	No Data !
IP			
No Data !			

- Click **Set IP** to display following window. This setup will delete an IP if there is no packet going through a computer (doesn't use network).



- Click **ISP** to display the Internet Service Provider of sniffed IP, and then click the link and icon of ISP field to display source's location.

No.	狀態	電腦 IP	電腦名稱	最後存在時間	ISP	群組
1.	<input type="checkbox"/>	203.119.190	***		GIGAMEDIA	GROUP1
2.	<input type="checkbox"/>	192.168.8.20	***		Intranet	GROUP1
3.	<input type="checkbox"/>	192.168.8.19	***		Intranet	GROUP1
4.	<input type="checkbox"/>	192.168.8.18	***		Intranet	GROUP1
5.	<input type="checkbox"/>	192.168.8.15	***		Intranet	GROUP1
6.	<input type="checkbox"/>	192.168.8.14	***		Intranet	GROUP1
7.	<input type="checkbox"/>	192.168.8.13	***		Intranet	GROUP1
8.	<input type="checkbox"/>	192.168.8.12	***		Intranet	GROUP1
9.	<input type="checkbox"/>	192.168.8.11	***		Intranet	GROUP1

2. List of Logged-in Users

You may check logged-in users for security management.

The screenshot displays a web-based network management interface. On the left is a sidebar menu with various system management options. The main content area shows a table of logged-in users. At the top of the main area, there is a status bar indicating disk usage: '硬碟資訊: 大小 - 109G / 已使用 - 1.2G / 剩餘空間 - 102G / 剩餘空間 (%) - 98%'. Below this, there are tabs for '線上 IP 資訊', '登入使用者清單', and '網域'. The '登入使用者清單' tab is active, showing a table with 10 rows of user login data. The table columns are 'No.', 'IP', '使用者名稱', and '時間'. Below the table, there is a pagination control showing '共 10 筆, 共 1 頁, 目前在第 1 頁 | 每頁顯示: 20' and a '送出' button. At the bottom left, there is a search bar with the text '全文檢索' and a '查詢' button.

硬碟資訊: 大小 - 109G / 已使用 - 1.2G / 剩餘空間 - 102G / 剩餘空間 (%) - 98%

線上 IP 資訊 登入使用者清單 網域

No.	IP	使用者名稱	時間↑
1.	192.168.8.19	root	2005-11-04 14:41:09
2.	192.168.8.11	root	2005-11-04 14:23:22
3.	192.168.8.13	root	2005-11-04 13:42:38
4.	192.168.8.19	root	2005-11-04 13:19:45
5.	192.168.8.11	root	2005-11-04 11:50:11
6.	192.168.8.19	root	2005-11-04 11:41:34
7.	192.168.8.11	root	2005-11-04 11:03:38
8.	192.168.8.18	root	2005-11-04 10:40:45
9.	192.168.8.19	root	2005-11-04 10:16:36
10.	192.168.8.11	root	2005-11-04 10:12:03

共 10 筆, 共 1 頁, 目前在第 1 頁 | 每頁顯示: 20 送出

刪除

版本: B0312.00:00
建議解析度為 1024x768

全文檢索

查詢

3. Nbns

NetBIOS Name Server (NBNS), the following UI records targets' NetBIOS name and group name in order to recognize the different people who might use the same IP addresses.

Hard Disk Information : - 73G / Used - 7.9G / Available - 61G / Available (%) - 88%

Online IP Info / Login User List / Nbns						
NO.	DATETIME↑	IP	MAC	NAME	GROUP	
1.	2007-04-20 11:03:12	192.168.1.143	00:15:00:4b:cb:ec	# Q YOUR-C950970BE1	#	
2.	2007-04-18 13:13:10	192.168.1.35	00:15:00:4b:cb:ec	# Q YOUR-C950970BE1	#	
3.	2007-04-16 11:54:10	10.0.0.3	00:30:1b:ae:71:64	# Q YOSHIKUN-6B1892	#	
4.	2007-04-14 18:47:19	219.76.92.157	00:14:78:11:d5:2d	# Q GW	#	
5.	2007-04-14 18:43:25	219.76.93.119	00:13:ce:75:7b:64	# Q	# 1__MSBROWSE__1	
6.	2007-04-14 18:41:26	219.76.93.15	00:13:02:1b:a6:28	# Q	# WORKGROUP	
7.	2007-04-14 18:36:20	219.76.93.185	00:0e:35:7a:e6:f9	# Q YOUR-BE77686312	#	
8.	2007-04-14 18:35:46	219.76.92.137	00:13:02:89:d7:d1	# Q NATALIE	#	
9.	2007-04-14 18:35:43	219.76.93.58	00:16:cf:b4:36:68	# Q LENOVO-3D904DDB	#	
10.	2007-04-14 18:32:04	219.76.92.205	00:16:ce:0a:39:41	# Q HADI-5265EF0196	# 1__MSBROWSE__1	
11.	2007-04-14 18:31:57	219.76.93.113	00:18:de:04:89:53	# Q OLIK	#	
12.	2007-04-14 18:31:25	219.76.93.185	00:0e:35:7a:e6:f9	# Q WORKGROUP	#	
13.	2007-04-14 18:30:25	219.76.92.99	00:11:6b:32:e5:30	# Q TANG-TOYD9608F5	#	
14.	2007-04-14 18:28:19	219.76.93.185	00:0e:35:7a:e6:f9	# Q YOUR-BE77686312	# 1__MSBROWSE__1	
15.	2007-04-14 18:26:14	219.76.92.92	00:18:de:04:63:e7	# Q YOUR-3725624587	#	
16.	2007-04-14 18:25:37	219.76.92.212	00:12:17:7d:3f:c4	# Q WORKSTATION3	#	
17.	2007-04-14 18:22:00	219.76.92.205	00:16:ce:0a:39:41	# Q HADI-5265EF0196	# MSHOME	
18.	2007-04-14 18:21:26	219.76.92.140	00:18:dec7:f8:07	# Q	# WORKGROUP	
19.	2007-04-14 18:21:26	219.76.92.205	00:16:ce:0a:39:41	# Q	# 1__MSBROWSE__1	
20.	2007-04-14 09:42:53	192.168.1.9	00:12:fd:15:c4:7f	# Q TONY	#	

Count : 134 , Total : 7 , In page 1 | Rows per page : 20 Submit

Features in this user interface (UI):

- [1] : # : To converter to convert the code in order to make characters readable.
- [2] : Q : The function to find out the information belonged to specific target.

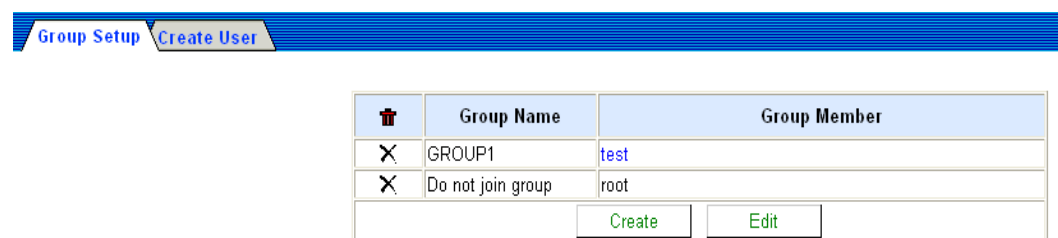
P. Authority Setup

It's divided into two parts:

1. Group setup
2. Create user

1. Group Setup

It includes create new group, change group name, add user, modify user; press Submit to activate settings after set up.

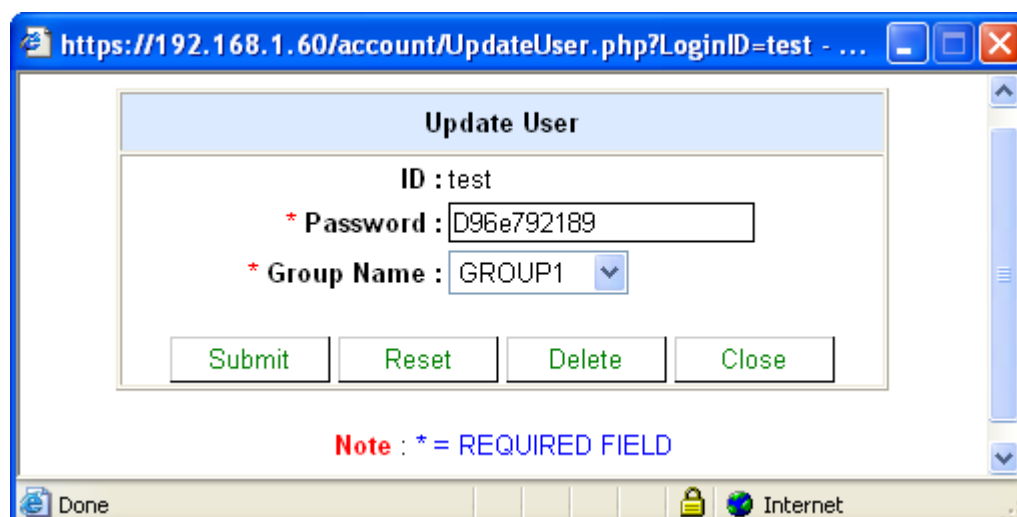


	Group Name	Group Member
X	GROUP1	test
X	Do not join group	root

Create Edit

Note : If this group has no members, then you can delete this group.

- Modify user's password, group and computer IP
Click on **Group member** to display the following window. Modify by the order, and then press **[Submit]**.



https://192.168.1.60/account/UpdateUser.php?LoginID=test - ...

Update User

ID : test

* Password : D96e792189

* Group Name : GROUP1

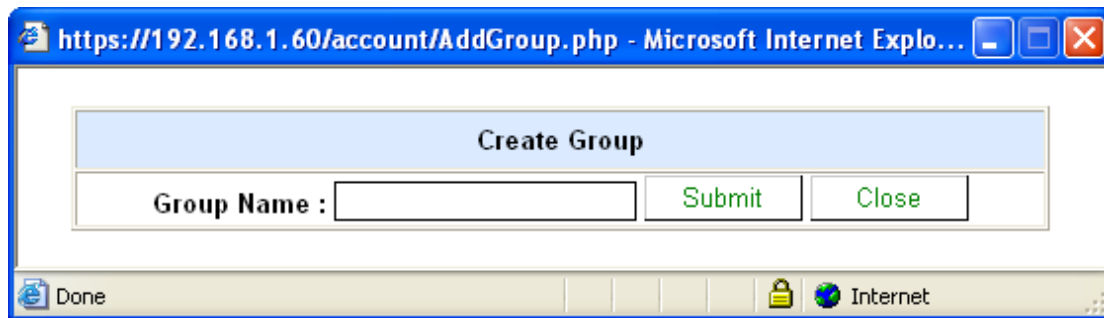
Submit Reset Delete Close

Note : * = REQUIRED FIELD

Done Internet

- Create new group

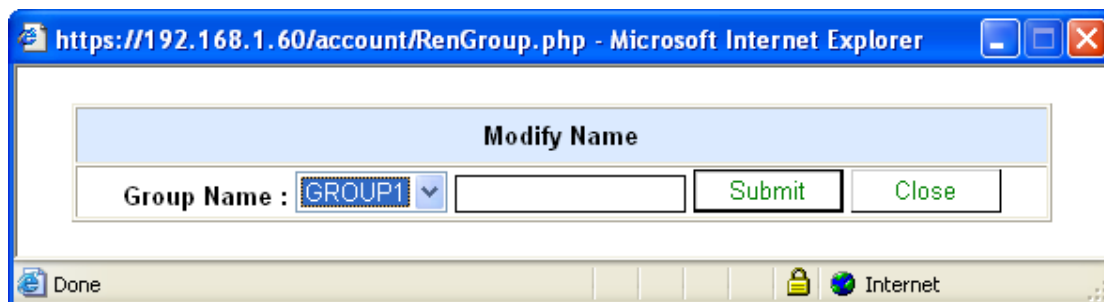
Input group name (can be in Chinese) and press **[Submit]**.



The screenshot shows a web browser window titled "https://192.168.1.60/account/AddGroup.php - Microsoft Internet Explo...". The main content area has a light blue header bar with the text "Create Group". Below this, there is a form with the label "Group Name :" followed by a text input field. To the right of the input field are two buttons: "Submit" and "Close". The browser's status bar at the bottom shows "Done" on the left and "Internet" on the right, with a lock icon in between.

- Change group name

Change group name (can be in Chinese) and press **[Submit]**.



The screenshot shows a web browser window titled "https://192.168.1.60/account/RenGroup.php - Microsoft Internet Explorer". The main content area has a light blue header bar with the text "Modify Name". Below this, there is a form with the label "Group Name :". This is followed by a dropdown menu currently showing "GROUP1", and then an empty text input field. To the right of the input field are two buttons: "Submit" and "Close". The browser's status bar at the bottom shows "Done" on the left and "Internet" on the right, with a lock icon in between.

2. Create user

- Create user

Input login account, password and group, then press **[Submit]**.

Group Setup		Create User	
Create User			
ID :	<input type="text"/>		
* Password :	<input type="password"/>		
* Group Name :	<input type="text" value="GROUP1"/> ▼		
		<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

Note : * = REQUIRED FIELD

Q. Delete Data

It is divided into two parts:

1. Delete (Mode)
2. Delete (All)

1. Delete (Mode)

Use drop-down list to select POP3, SMTP, FTP, MSN, ICQ, P2P, YAHOO, HTTP, HTTP (Dynamic), TELNET, WEBMAIL, WEBMAIL (Send) and etc. to be deleted. Date and time can also be specified. Column to be deleted can also be specified. Delete by pressing [Submit].

Delete (Mode)		Delete (All)	
Mode :	POP3		
Date / Time :		~	
Column :	IP		
Column Value :			
<input type="button" value="Submit"/>			

Note : Mode FTP => Column Action => Column Value Upload:0 Download:1

2. Delete (All)

Input user's account and password for delete all data.

Delete (Mode)

Delete (All)

Login User :

Login Pass :

Submit

R. EDIT PASSWORD

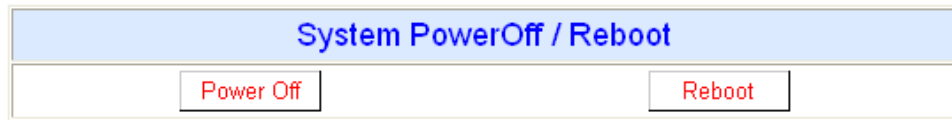
Input the new password; press the button [Submit] to set up.

Modify Userself Password	
ID :	root
* New Password :	<input type="text"/>
* Confirm Password :	<input type="text"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

Note : * = REQUIRED FIELD

S. POWER ON/OFF

This UI allows user to turn off or reboot the computer.

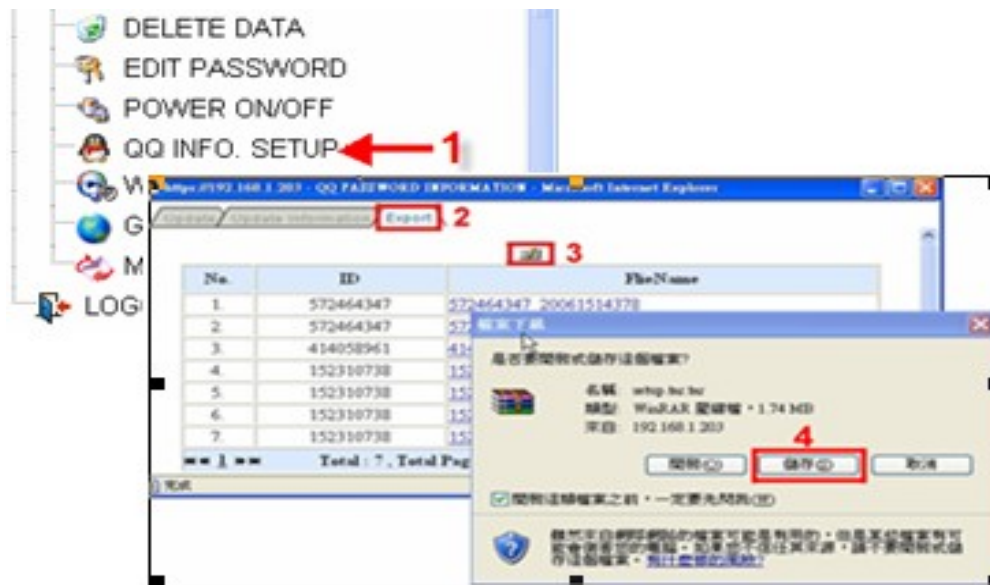


T. QQ INFO. SETUP (How to see the encrypted conversation)

The captured conversation in QQ will be all encrypted. This section tells users how to download the QQ cracker to decrypt the information.

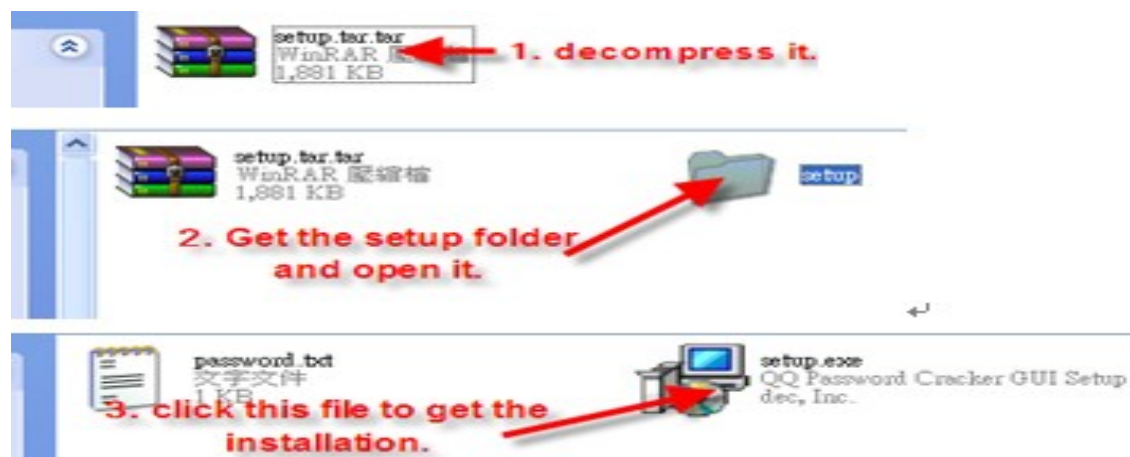
Step 1 – Download the QQ cracker:

The following diagram shows the steps to download the QQ cracker.

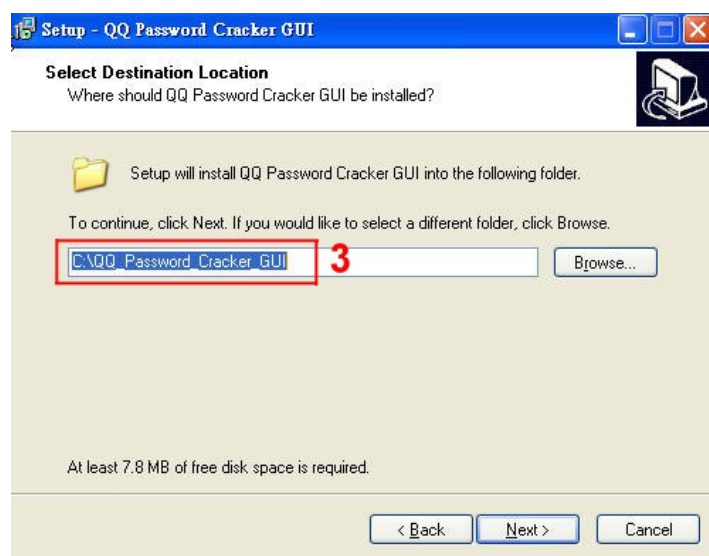
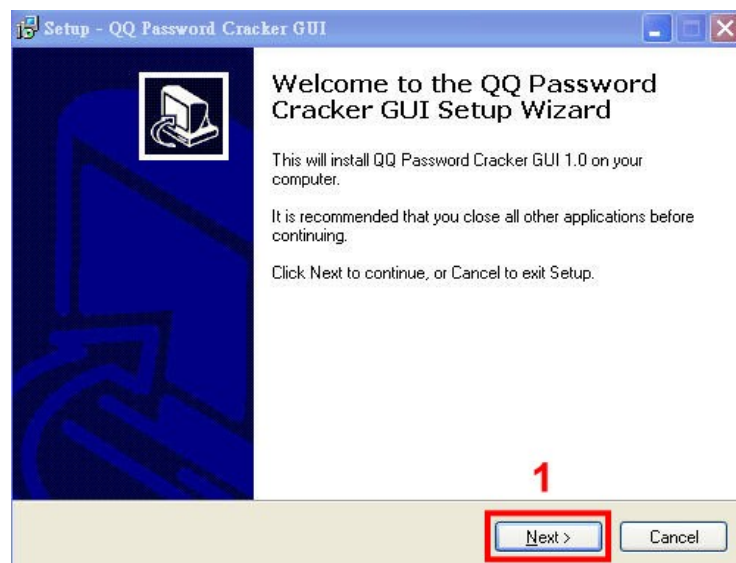


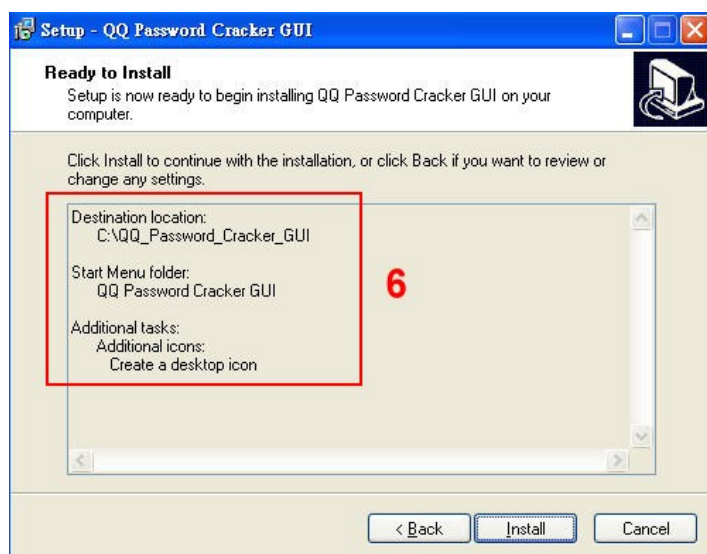
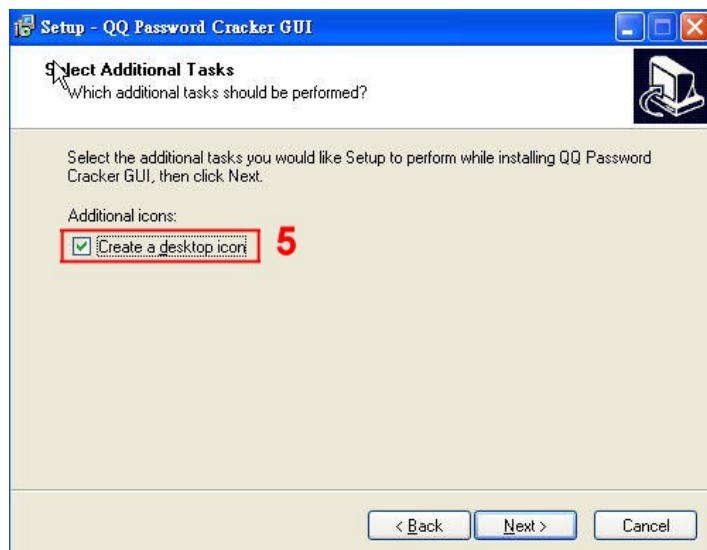
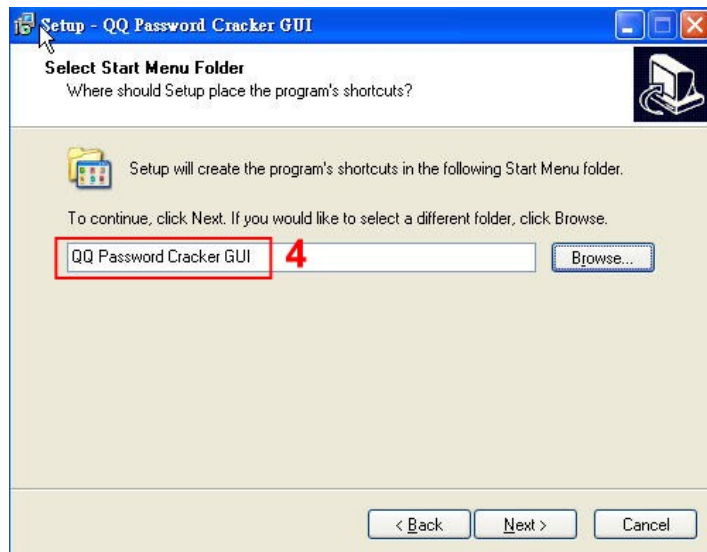
Step 2 – Install QQ cracker into computer.

Decompress the file called “setup.tar.tar” to get the folder called “setup”. Open it and press the setup.exe to get the installation.



The following diagrams show the steps of installation.





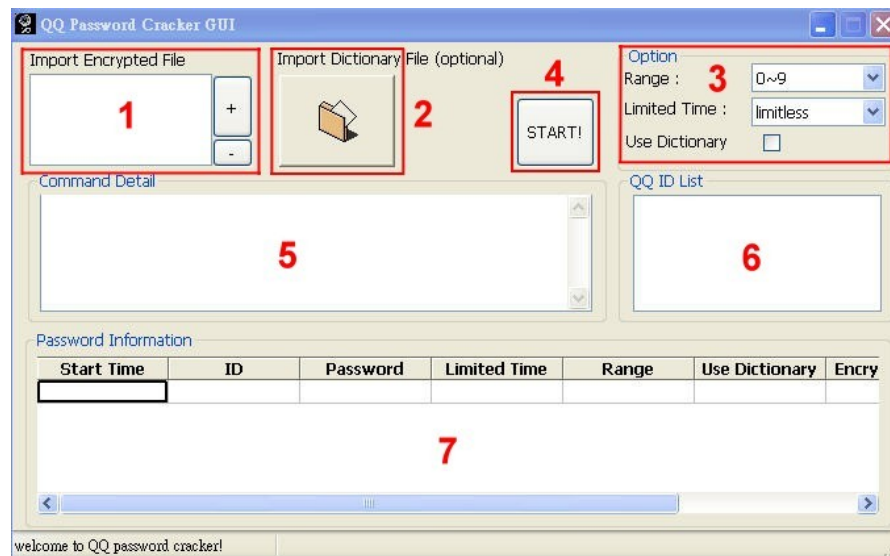


Step 3 – Decrypt the conversation.

Go to Export page to download the decrypted conversation file.



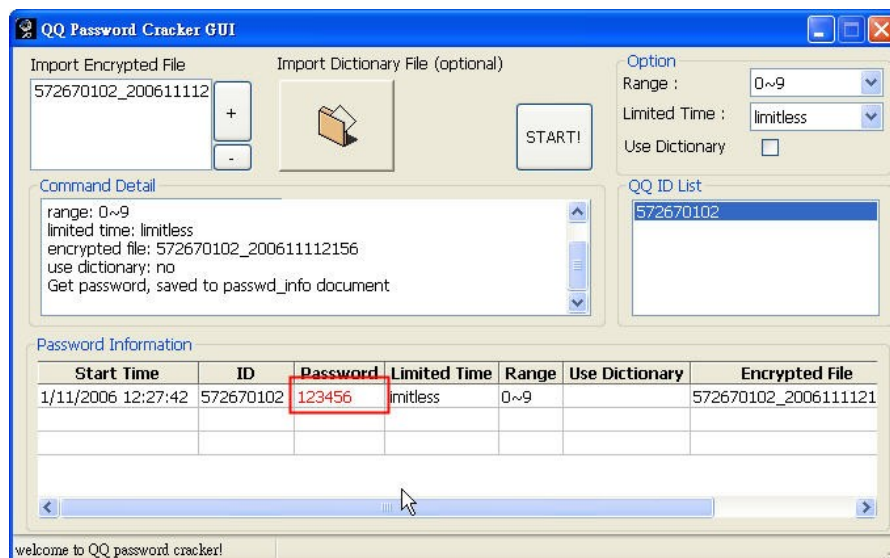
Run the QQ cracker and import the decrypted file you just download at the previous step.



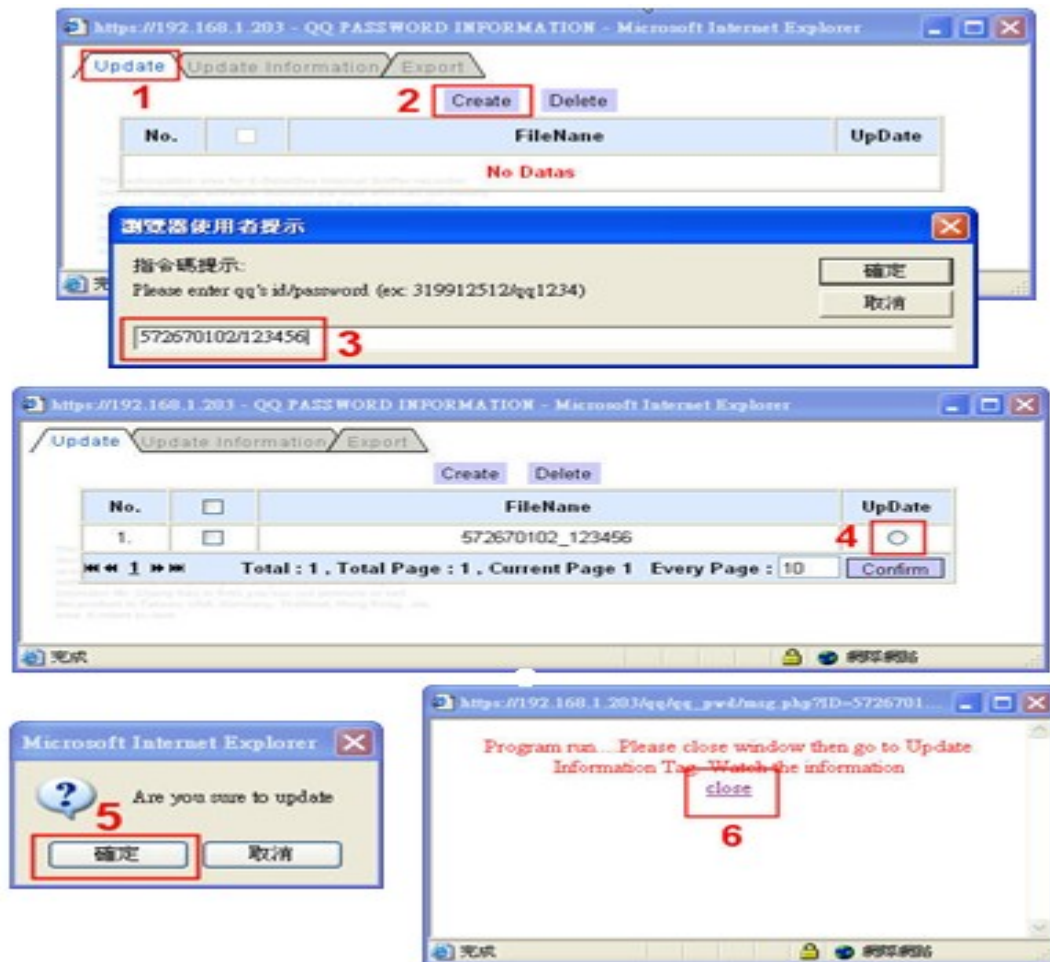
Item	statement	
1	Import Encrypted File	Choose + or - button, add or remove to run files.
2	Import Dictionary File	Dictionary file records the general passwords which people may use. If you have own dictionary file, you can import it into this cracker when you decrypt the conversation.
3	Option	Range – Setup the possible combinations of password.

		<p>Limited Time – Setup the max time to get the key. Even if this cracker does not still get the password for you, the process will be stopped when time is out.</p> <p>Use Dictionary – Cracker uses the dictionary's information to do the password matching if the checkbox is ticked.</p>
4	START	Start to run program button.
5	Command Detail	Show procedure for detailed information.
6	QQ ID List	Shows the history of QQ ID records.
7	Password Information	Shows the findings if password is found.

Get the password as shown in the following diagram.



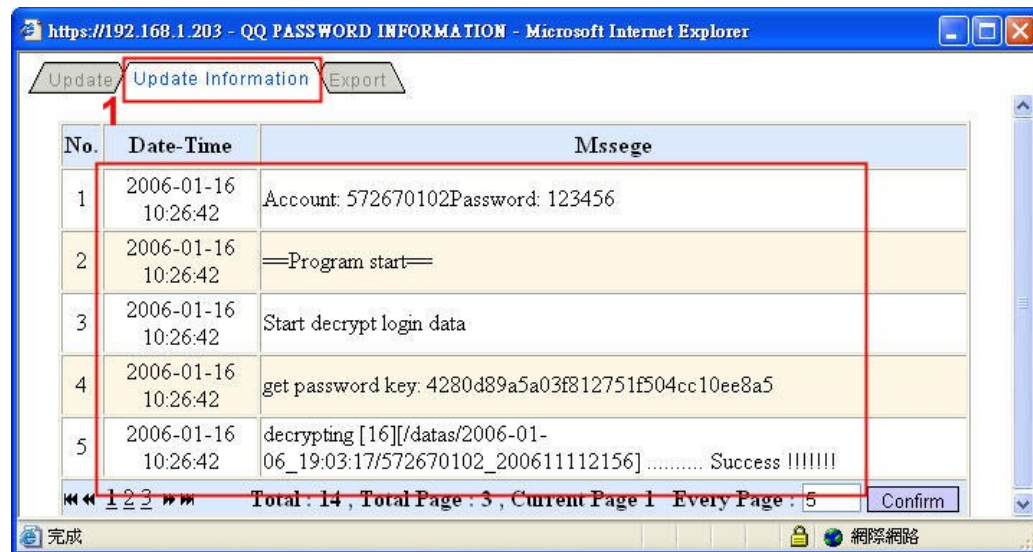
The section illustrates how to decrypt the decrypted file in order to see its conversation with the following diagrams. (input the ID & password)



And then you can actually be able to see the conversation content.

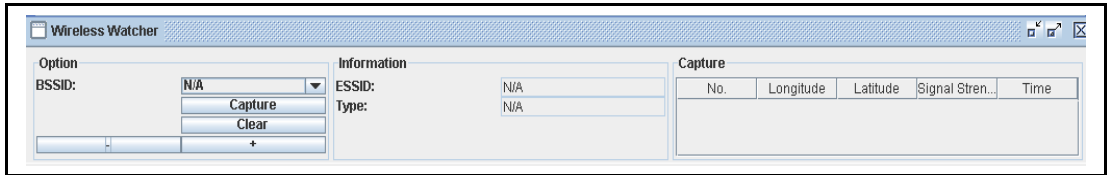


The update page shows the decrypting procedures.



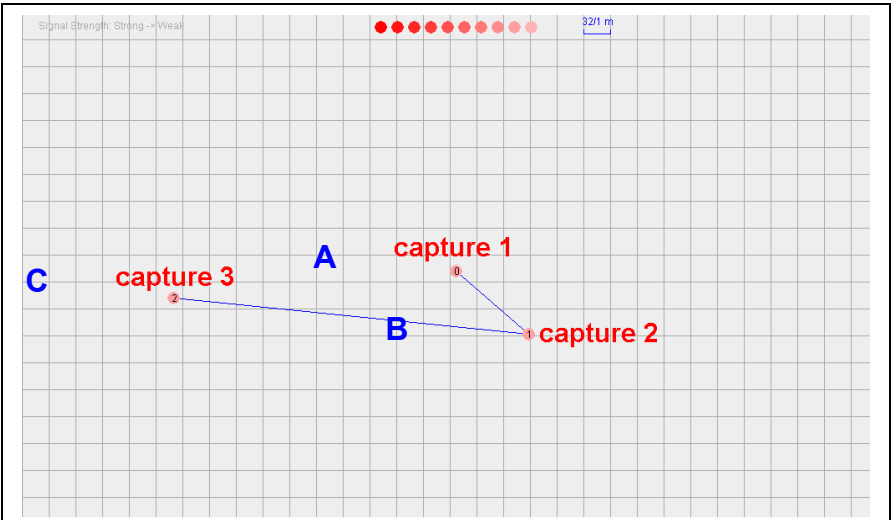
U. GPS

GPS function allows administrator to approximate the location of APs or STAs.



Option		Information		capture	
BSSID	BSSID key	ESSID	ESSID key	No	Number
Capture	Capture location	Type	AP or PC	Longitude	Longitude
Clear	Clear location			Latitude	Latitude
+	Zoom in			Signal Strength	Signal Strength
—	Zoom out			Time	Time

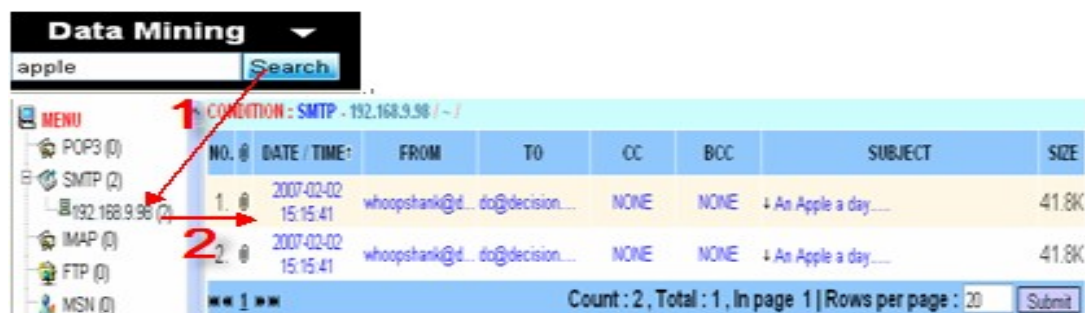
Refer to the diagram below. When wireless e-detective system with GPS moves and stops at location A, press Capture. The GPS diagram can set the location of A as Capture 1. When E-detective system moves to location B and C, press Capture at each location and the system will record these two locations as Capture 2 and Capture 3. Just move the mouse arrow to the captured location, and it will display the location information.



V. Data Mining



E-Detective full text search of **Data Mining** let you use searching criteria to match user's input keyword. The system will match keyword with text and attachment of numerous e-mails (E-mail / POP3, SMTP, IMAP, Hot-Mail, Web-Mail), which stored in database, then list the mail, which meets keyword criteria.

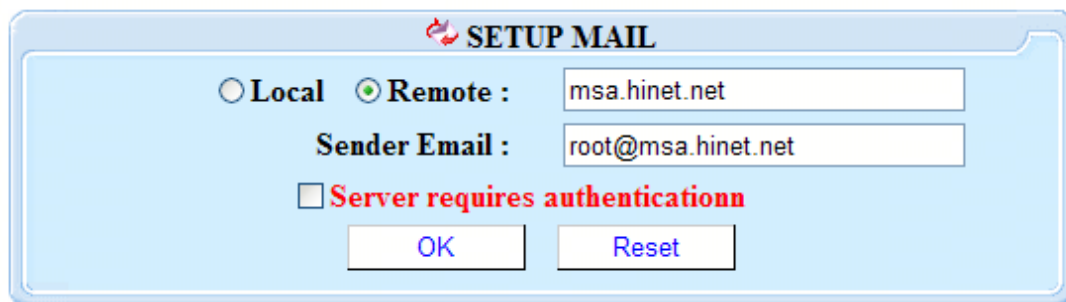


X. Mail Setup

The system can send alert email to administrator or users by setting up the mail system.

Setup instruction:

1. Enter the remote or local mail server. For example: msa.hinet.net
2. Enter the Sender Email address. For example: xxx@msa.hinet.net.



SETUP MAIL

☐ Local ☒ Remote : msa.hinet.net

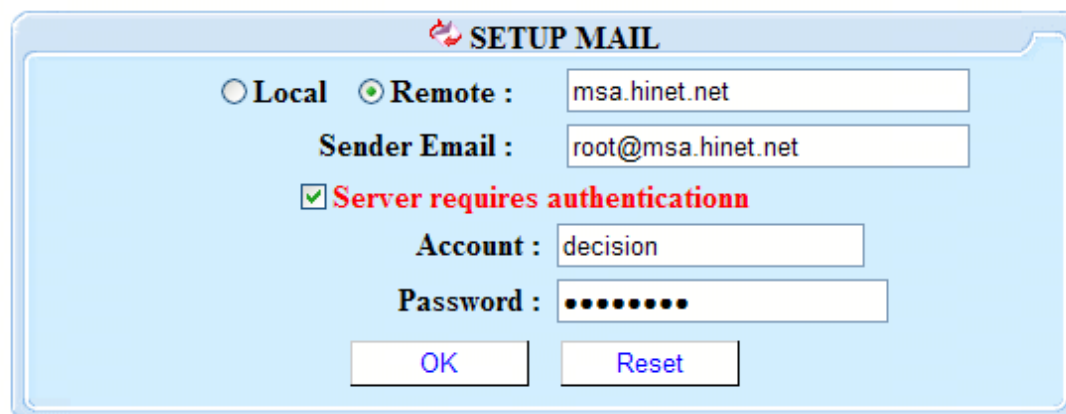
Sender Email : root@msa.hinet.net

☐ **Server requires authenticationn**

OK Reset

Server requires authentication:

If server authentication is needed, please input the server account and password and click [OK].



SETUP MAIL

☐ Local ☒ Remote : msa.hinet.net

Sender Email : root@msa.hinet.net

☒ **Server requires authenticationn**

Account : decision

Password :

OK Reset

Appendix A: Q & A

Note: local machine means where E-Detective situated with monitor and keyboard connected.

- After installed, what should I do if I couldn't see the computer data to be captured?

答 : 1. Confirm if you've registered. If yes, then excute program [OpenRaw].

Please type the following command in local machine.

```
edetective:/# ps -x | grep OpenRaw
```

[[|] refers to the shifted key of [\] in your keyboard

If [OpenRaw] correctly execute, you should be able to read the following messages:

```
./OpenRaw -t /datas/rawdata -i ethX
```

```
./OpenRaw -t /datas/rawdata -i ethX
```

```
./OpenRaw -t /datas/rawdata -i ethX
```

```
./OpenRaw -t /datas/rawdata -i ethX
```

```
./OpenRaw -t /datas/rawdata -i ethX
```

```
./OpenRaw -t /datas/rawdata -i ethX
```

2. Please confirm if the system has recognized PCI WatchDog Card of Decision Computer International Co.while system booting.

Please type the following command in local machine.

```
edetective:/# lspci -n | grep 6666
```

[[|] refers to the shifted key of [\] in your keyboard

If PCI WatchDog Card is correctly installed, you should be able to read the following messages:

```
Class XXXX : 6666 : 4100 [ EXXX ]
```

3. Please confirm if there is any data in on-line IP information of network user list.

- How to change IP?

Ans: Local machine: please refer to manual P.7 ~ P.9

Remote: please refer to manual P.10

- How to install hardware? Which mode will meet my needs?

Ans: please refer to manual P. 4

Copyright © 2007 Decision Computer International Co., Ltd

Note: if you are installing Mirror mode, your Switch Hub must have Mirror Port function.

- How to record data from different network segment?

Ans: please refer to manual P.74

- Can't back up or burn CD?

Ans: Please make sure CD-ROM drive is correctly installed at 1st socket of IDE2 (or 2nd flat cable).

- The file extension of uploaded and downloaded file captured by FTP is *.txt?

Ans: Right-click to **Save as** another file, change it to correspondent file extension, and then open it.

Ex.: *.jpg, *.pdf, *.rar, etc.

- MSN or ICQ can't capture data?

Ans: Turn on 1863 port of firewall.

Turn on 5190 port of firewall.

- Can't use Web interface after booting system?

Ans: It has used 443 port; please use <https://192.168.1.60> to log in. (default E-Detective IP is 192.168.1.60)

- If I've used Proxy, the IP in Web log belongs to Proxy. Is it correct?

Ans: Yes, you can only have Proxy's data. (If E-Detective is installed in front of Proxy)

- How do user interfaces arrange themselves automatically and save the settings after arranged without rearrange next time? What's the right size of background graphic to fit screen?

Ans: 1. After arranged the positions, right-click on the icon of user interface and choose **Save current settings** to save the position.

2. There is no size limit on background graphic; it depends on your screen resolution.

- Warning policy doesn't work after setting up, and system doesn't send a warning letter to the specified receiver?

Ans: It's scheduled to execute one hour after setting up, please refer to **Copyright © 2007 Decision Computer International Co., Ltd**

manual P.50 for policy setup.

- Can't directly open and view mail in POP3 / SMTP?

Ans: Go to **Control Panel** -> **Add / Remove Program** and check if there is any **Outlook Express** Updates; if yes, please remove it.